МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ І СПОРТУ УКРАЇНИ
ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА КВАНТОВОЇ ЕЛЕКТРОНІКИ

ШУАІБОВ О. К.

ОРГАНІЗАЦІЙНА РОБОТИ З ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ (ПРАКТИКУМ)

Навчальний посібник для самостійної роботи студентів з напрямку підготовки **6.170102 - "Системи технічного захисту інформації"**, галузь знань **1701 «Інформаційна безпека»**

Ужгород-2011

ББК. 32.973я73
Г 14
УДК 004.056. 5(075.8)

Організаційна робота із захисту інформації в інформаційно-комунікаційних системах (практикум). Навчально-методичний посібник для самостійної роботи студента з курсу за вибором //Шуаібов О. К. - Ужгород, ДВНЗ «УжНУ», «Говерла». **2011**. – **98** с.- Іл.: **4** . - Бібл.: **9** назв. – Укр. мовою. - 2011 р.

Навчальний посібник написано у відповідності до вимог тимчасового Положення ДВНЗ «УжНУ» стосовно Болонського процесу до навчальних дисциплін і призначений для курсу «**Організаційно-технічне забезпечення систем захисту інформації»**, який вивчається студентами, що спеціалізуються на кафедрі квантової електроніки. Він містить матеріал до чотирьох практичних робіт з організаційних питань захисту інформації в автоматизованих системах, питання модульного котролю, тести до десяти контрольних робіт, теми рефератів та список літератури з даної навчальної дисципліни.

Посібник покликаний сприяти більш якісній підготовці студентів до практичних робіт, оскільки містить теоретичний матеріал до них та відповідні методичні матеріали, що важливо для більш повного засвоєнню знань і одержання практичних навиків студентами з методів організаційного захисту інформації в автоматизованих системах

Навчальний посібник призначений для використання студентами, що спеціалізуються в галузі захисту інформації та безпеки інформаційно-комунікаційних систем.

Рецензент: доктор фіз.-мат. наук, професор, завідувач кафедри твердотільної електроніки **Різак Василь Михайлович** ДВНЗ «Ужгородський національний університет».

Рекомендовано до друку методичною комісією фізичного факультету ДВНЗ «УжНУ», протокол № від березня 2011 р.

ЗМІСТ

ПЕРЕДМОВА

Більшість інформації становить певну цінність, тому інформаційні ресурси потребують захисту від різних впливів, які можуть знизити її цінність. Завдання захисту інформації, переважно державних і військових таємниць, було досить актуальним і незмінним на протязі тисячоліть – забезпечення передавання інформації від достовірного джерела вповноваженій особі так, щоб вона не потрапила до інших осіб.

У XX – столітті правила роботи з таємною інформацією, способи її збереження та передавання зазнали значних змін через бурхливий розвиток технічних засобів, які широко використовуються як для захисту інформації, так і для подолання цього захисту.

В кінці XX століття відбулась чергова технічна революція з підготовки, зберігання, пошуку, оброблення та поширення інформації з використанням комп`ютерної техніки, комп`ютерних мереж (в тому числі і глобальних). В результаті цього були розроблені і стали широко використовуватись розподілені інформаційні системи, які назвали інформаційно-комукаційними.

Питання захисту цифрової інформації з однієї сторони можна вирішувати так же, як і для захисту традиційних (паперових) носіїв інформації, а з другої сторони, використання комп`ютерних технологій обробки інформації несе і нові загрози. Зокрема, це використання шкідливого і навіть руйнівного програмного забезпечення (комп`ютерні віруси). Тому задачі захисту інформації в інформаційно-комукаційних системах є суперпозицією двох напрямків:

- захист важливої інформації, зокрема, державної, військової або комерційної таємниці, від цілеспрямованого втручання;
- захист інформації від впливів, спричинених некоректним функціонуванням комп`ютерної системи через відмови обладнання, збої в роботі

програмного забезпечення, помилки в реалізації апаратних або програмних засобів, чи наявність програмних засобів з прихованими руйнівними властивостями.

В даному навчально-методичному посібнику розглянуто чотири теми практичних робіт з організаційної роботи із захисту інформації в інформаційно-комунікаційних системах, які виконуються на протязі першого модуля дисципліни та основні методичні матеріали.

Матеріали навчального посібника базуються на попередньо вивченій студентами дисципліні “Безпеки життєдяльності” і підготовлені з метою сприяння в забезпеченні високого рівня підготовки студентів з безпеки інфомаційно-комунікаційних систем.

Питання та методичні матеріали посібника закладають студентам фундамент для подальшого засвоєння знань із дисциплін, в яких вивчається захист інформації в комп`ютерних системах з використанням программних методів захисту інформації, основ криптографії та документознавства в галузі захисту інформації.

Тема – 1 ОРГАНІЗАЦІЙНА РОБОТА ІЗ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В КРАЇНАХ НАТО І ЄС

1. **Мета роботи.**

Ознайомлення з основами організаційної роботи із захисту інформації з обмеженим доступом у країнах НАТО і ЄС в розрізі відповідних мінімальних стандартів. Засвоєнння термінів інформаційної безпикикраїн НАТО і ЄС; основні положення документа С-М(2000) 49; базові принципи захисту та ступені секретності інформації в країнаї Європи;

2. **Необхідна література.**

Стандарти захисту інформації з обмеженим доступомв країнах Нато і ЄС.;

В.С. Сідак, В.Ю. Артемов Забезпечення інформаційної безпеки в країнах НАТО тп ЄС: Навчальний посібник. К.: КНТ. 2007. 160 с.

3. **Основні теоретичні відомості.**

3.1. Термінологія.

Зміст наступних термінів (в Україні):

«національна безпека» - це стан захищеності гарантованих законодавством умов життєдіяльності держави, суспільства та окремої особи від внутрішніх та зовнішніх загроз;

«інформаційна безпека» - складова національної безпеки, що характеризує стан захищеності встановлених законодавством норм і параметрів інформаційних процесів та відносин і забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин;

«організаційно-правові основи інформаційної безпеки» - це нерозривна єдність організаційних методів та правових норм регулювання суспільних відносин, що виникають з приводу встановлення режимів і параметрів суспільного обігу інформації, правового статусу, поведінки та зв'язків суб'єктів інформаційних процесів.

Захист інформації з обмеженим доступом є головним завданням системи забезпечення національної безпеки України.

Основні принципи захисту інформації з обмеженим доступом, або ***за термінологією НАТО*** — **політика інформаційної безпеки SOI** (Security Of Information Policy), регулюються документом С-М(2002)49 «Ключові питання інформаційної безпеки НАТО», С-М(2002)50 «Захист проти загроз тероризму» та С-М(2002)60 «Поводження з некласифікованою інформацією НАТО».

Аналіз документів Альянсу свідчить, що в термінології НАТО відсутнє поняття «інформація з обмеженим доступом». Навпаки, НАТО поділяє всі документи на «класифіковані» (classified), тобто такі, для яких визначено рівень обмеження доступу і які внесені до відповідних реєстрів, та «некласифіковані» (unclassified), які до відповідних реєстрів не внесені, але доступ до яких обмежується. Поводження з інформацією НАТО, яка має класифікацію «NATO Unclassified», регулюється документом С-М(2002)60.

3.2. П'ять інституційних принципів, покликаних забезпечити високий рівень інформаційної безпеки:

широта (Breadth), глибина (Depth), централізація (Centralization), контрольований доступ (Controlled Distribution), персональний контроль (Personnel Controls).

Сутність захисту інформації НАТО з обмеженим доступом полягає у використанні наступних принципів:

уніфікації рівнів класифікації інформації в НАТО і національних системах захисту інформації країн-учасниць;

варіативності, який полягає у тому, що НАТО не нав'язує країнам-членам норми і способи захисту інформації з обмеженим доступом, надаючи їм право обирати власні шляхи;

автентичності, надання рівня класифікації інформації з обмеженим доступом;

збереження рівня класифікації інформації;

доцільності надання доступу до інформації НАТО фізичним особам;

перевірки благонадійності фізичних осіб для надання їм допуску до інформації з обмеженим доступом;

інституційованого моніторингу системи забезпечення захисту інформації з обмеженим доступом в НАТО і країнах-учасницях.

Принцип **відповідності** норм захисту інформації з обмеженим доступом у НАТО і національному законодавстві країн-учасниць означає, що держави-члени НАТО беруть зобов'язання регулювати на основі єдиних стандартів доступ не лише до інформації, яка належить НАТО, а й до всіх видів інформації, обов'язки щодо захисту якої бере на себе держава-учасник.

Принцип **автентичності** надання рівня класифікації інформації з обмеженим доступом полягає в тому, що лише той орган країни-члена НАТО, який є автором документа, має право надавати йому ступінь секретності або — у термінології НАТО — рівень класифікації.

Принцип **доцільності надання доступу до інформації фізичним особам** у НАТО також вважається фундаментальним. У термінології НАТО він носить назву *потреба знати (need-to-know)* і полягає в тому, що фізичні особи повинні мати доступ до класифікованої інформації лише якщо вони мають потребу в такій інформації для виконання їх прямих службових обов'язків, і доступ ніколи не має надаватися тільки тому, що особа обіймає певну службову посаду.

Принцип **перевірки благонадійності фізичних осіб** для надання їм допуску до інформації з обмеженим доступом вбачає правила щодо відбору осіб, які мають право одержати доступ до інформації з обмеженим доступом. Відповідно до цього принципу контроль заснований на перевірці благонадійності (характеру та способу життя) кандидатів на доступ до класифікованої інформації. Кандидати повинні демонструвати лояльність, відповідний характер, звички та спосіб життя, який без сумніву заслуговує на довіру.

Принцип **інституційованого моніторингу** системи забезпечення захисту інформації з обмеженим доступом в НАТО і країнах -учасницях означає вимогу мати в кожній державі-члені НАТО інституційований національний уповноважений орган або урядове бюро національної безпеки (national security organization — NSO), яке відповідає за інформаційну безпеку та персонал, а також за збір і реєстрацію відомостей щодо шпигунства та підривної діяльності.

3.3.Ступені екретності.

Відповідно до політики безпеки НАТО, викладеної в історичному документі C-M(55)15(Final), а потім підтвердженої в документі C-M(2002)49 від 2002 р., існують такі рівні класифікації документів НАТО за ступенями таємності:

NATO TOP SECRET (NTS);
NATO SECRET (NS);
NATO CONFIDENTIAL (NC);
NATO RESTRICTED (NR).

На даний час затверджено наступний порядок, відповідно до якого встановлено такі ступені секретності:

COSMIC TOP SECRET (CTS) — несанкціоноване розкриття інформації з таким грифом може завдавати надзвичайно великої шкоди НАТО;

NATO SECRET (NS) — несанкціоноване розкриття інформації з таким грифом може завдавати дуже великої шкоди НАТО;

NATO CONFIDENTIAL (NC) — несанкціоноване розкриття інформації з таким грифом може завдати шкоди НАТО;

NATO RESTRICTED (NR) — несанкціоноване розкриття інформації з таким грифом може завдати шкоди інтересам або ефективності діяльності НАТО.

Для інформації категорії NATO ATOMAL встановлені грифи:

а) **COSMIC TOP SECRET ATOMAL;**

б) NATO SECRET ATOMAL;
в) NATO CONFIDENTIAL ATOMAL.

3.4. Структура додатку В документа С-М(2002)49.

Зміст захисту інформації з обмеженим доступом визначається стандартами НАТО. Мінімальні стандарти НАТО щодо захисту інформації з обмеженим доступом викладено у додатку В документа С-М(2002)49, який спирається на наступні директиви:

У НАТО під ***стандартизацією*** розуміють процес формулювання, узгодження, застосування та удосконалення стандартів з метою підвищення ефективності його діяльності. Аналіз організаційно-правових документів дає право стверджувати, що політика безпеки НАТО спирається на дуже розгалужену систему стандартів.

В Альянсі діє система стандартів **STANAG** (Standardization Agreement), яка містить три види стандартів: ***матеріальну частину, операційні та адміністративні.***

Стандартизація матеріальної частини включає розробку практичних посібників та технічних умов на перспективну та наявну техніку, в тому числі на засоби і системи, що забезпечують захист інформації з обмеженим доступом. Стандарти STANAG на нематеріальну частину підрозділяються на операційні (operational) та адміністративні (administrative).

Операційні стандарти STANAG поширюються на тактичні концепції, доктрини, методи, матеріально-технічне забезпечення, навчання особового складу, організаційні питання тощо.

Адміністративні стандарти STANAG частіше стосуються термінології. Вони застосовуються як в операційній, так і у матеріальній сферах. Ця категорія включає воєнні та невоєнні стандарти, які можуть бути корисними для поліпшення взаємодії в адміністративній роботі.

Кожна країна НАТО ратифікує STANAG та імплементує його до національної системи стандартів. Це робиться для

того, щоб кожна країна-член НАТО могла використовувати у воєнних цілях склади та технічну підтримку будь-якої іншої країни-члена НАТО.

3.5. Органи безпеки НАТО.

Органами безпеки НАТО є:
- офіс безпеки НАТО (NOS);
- органи безпеки у військових структурах НАТО (NAMILCOM);
- національні уповноважені органи по безпеці НАТО (NSA).

Структура органів безпеки НАТО наведена на рис.1.

Національний уповноважений орган з безпеки інформації (NSA) зобов'язаний забезпечувати наступне :
- безпеку інформації з обмеженим доступом у військових і цивільних органах і структурах у країні та за її кордонами;
- керівництво створенням або ліквідацією режимно-секретних органів (РСО), про відповідні дії щодо таких органів повідомляється NOS;
- проведення спільно з NOS періодичних інспекцій з перевірки виконання правил захисту інформації з обмеженим доступом у національних організаціях усіх рівнів — як військових, так і цивільних;
- перевірку відповідно до правил НАТО благонадійності всіх громадян своєї країни, які за родом своєї діяльності допущені до інформації з обмеженим доступом;
- розробку планів захисту інформації у надзвичайних обставинах для запобігання нелегітимному використанню інформації з обмеженим доступом, потраплянням її до чужих рук або до рук супротивника.

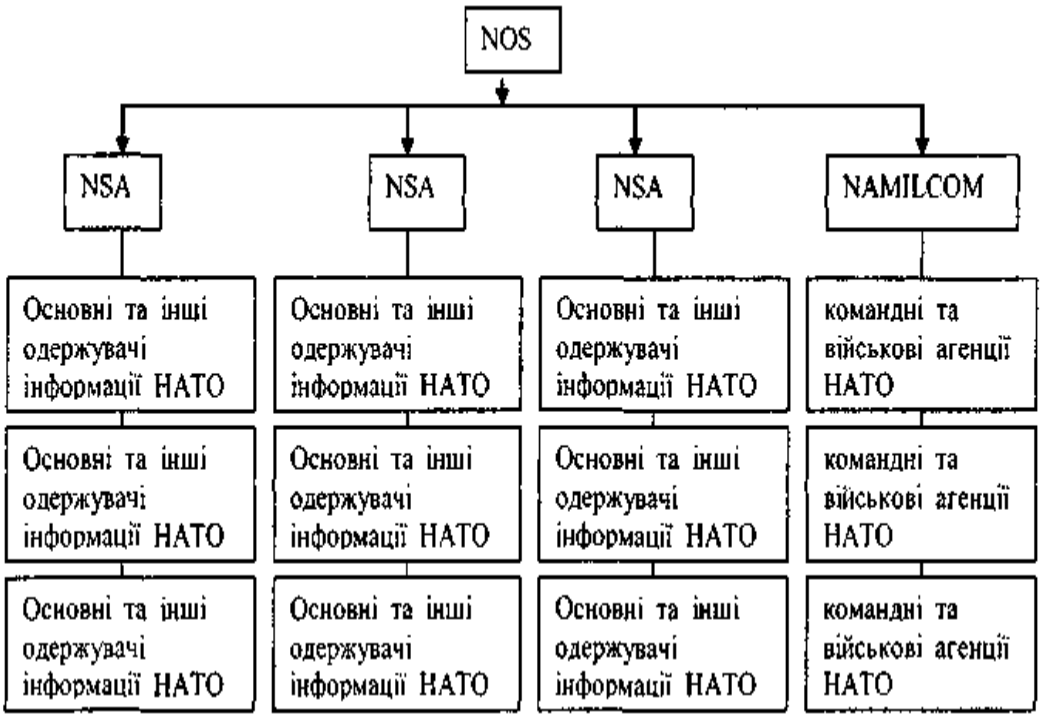

Рис. 1. Органи безпеки НАТО.

Структура і функції NOS наведені на рис.2.

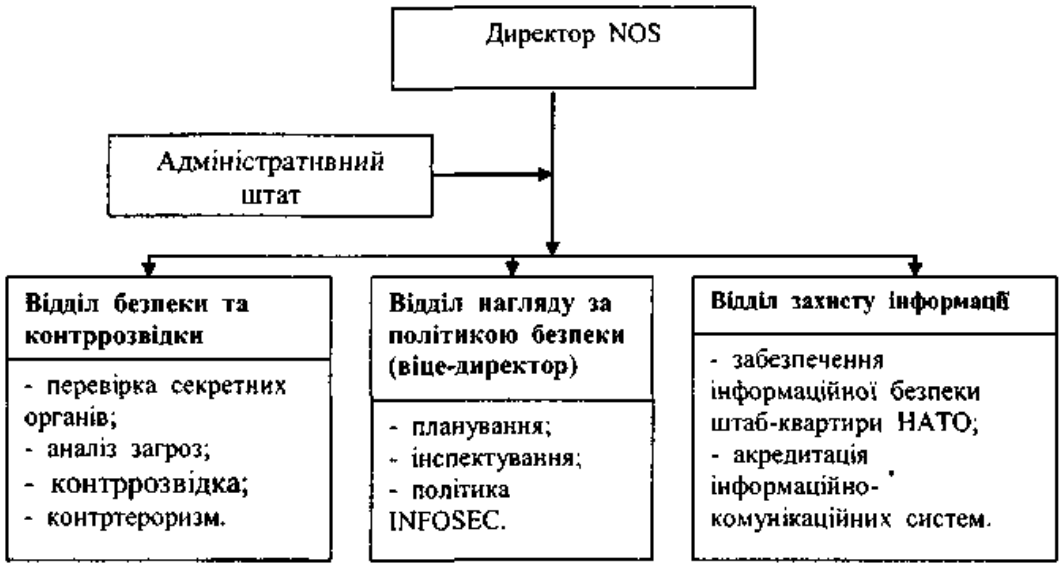

Рис.2. Структура NOS

3.6. Принципи та мінімальні стандарти політики безпеки НАТО.

Базові принципи та мінімальні стандарти політики безпеки НАТО стосуються наступних питань:створення системи надійних органів безпеки; організації захисту інформації, виробів, територій та споруд; забезпечення доступу до класифікованої інформації лише ретельно перевіреного персоналу.

До складу додатка **В документа С-М(2002)49**, який проголошує мінімальні стандарти НАТО у сфері захисту інформації з обмеженим доступом, входять такі розділи:
цілі і наміри; застосування; повноваження; основні принципи; фізична безпека; безпека персоналу; захист інформації; INFOSEC; промислова безпека; відповідальність за безпеку; національний орган безпеки (NSA); повноважний орган безпеки (DSA); комітет безпеки НАТО (NSC); офіс безпеки НАТО (NOS); військовий комітет NAMILCOM та військові організації НАТО**;** цивільні організації НАТО.

Заходи фізичної безпеки НАТО (Physical Security) передбачають: захист приміщень та споруд; захист інформації усередині приміщень та споруд; контроль доступу до приміщень та споруд; захист проти візуального спостереження та прослуховування.

При визначенні який саме ступінь фізичної безпеки у кожному конкретному випадку необхідний, беруться до уваги такі фактори: рівень класифікації і категорія інформації; кількість і форма збереження інформації; сертифікат допуску і необхідний для роботи рівень обізнаності персоналу; оцінка на місцевості загроз з боку спецслужб інших держав, терористичної або іншої кримінальної діяльності.

У якості заходів забезпечення **фізичної безпеки визначені такі**: огорожа по периметру та система охоронного освітлення; система виявлення порушника (IDS), у тому числі система відеоспостереження (CCTV); система контролю входів і виходів (електронна, електромеханічна або

фізична, тобто така, що здійснюється спеціально підготовленими охоронцями).

Фізична безпека визначає засоби захисту класифікованої інформації від технічних атак, наприклад, прослуховування. Офіси або територія, у яких класифікована інформація із грифом «SECRET» і вище регулярно озвучується, захищається від пасивного та активного прослуховування за допомогою надійних заходів фізичної безпеки з урахуванням виправданого ризику. Відповідальність за визначення такого ризику покладається на відповідні органи з питань безпеки й узгоджується з технічними спеціалістами.

Заходи щодо безпеки персоналу (Personnel Security) полягають в тому, що особи, яким санкціоновано доступ до інформації з грифом «Таємно» і вище, повинні пройти відповідну перевірку на допуск персоналу (Personnel Security Control — PSC), що проводиться органом національної безпеки або іншим уповноваженим органом. Процедури видачі сертифіката допуску здійснюються відповідно до політики безпеки НАТО і відповідних директив.

Рис.3. Система маркірувань класифікованих документів НАТО.

Безпека інформації (Information Security) передбачає нормування таких процедур поводження з документованою інформацією, які виникають при її: маркіруванні, класифікації, підготовці, обігу, включаючи розповсюдження (release), передачі на відстань; знищенні.

3.7. форми розповсюдження інформації в країнах НАТО.

Існують такі ***форми розповсюдження (release) інформації НАТО***: спорадичне розповсюдження та регулярне (планове) розповсюджування.

Нерегулярне надання інформації стосується спеціально відмічених документів.

Регулярне надання інформації може стосуватися існуючих документів або тих документів, які будуть створені. Це надання стосується лише категорій документів, а не конкретних документів. Однак категорії документів мають бути визначені із максимальною точністю (предмет, рівень класифікації, джерело тощо).

3.8. Вимоги щодо промислової та індустріальної безпеки

Вимоги щодо **промислової безпеки (Industrial Security**) унормовують порядок виконання промислових контрактів, які виконуються за замовленнями НАТО. Умови промислової безпеки містять: умови проведення переговорів й отримання дозволу на укладання засекречених контрактів з НАТО; вимоги безпеки щодо класифікованих контрактів НАТО; порядок оприлюднення наявної в контрактах класифікованої інформації НАТО; порядок перевірки промислової безпеки для контрактів НАТО; умови отримання підприємством ліцензій (FSC) на виробництво продукції та послуг за контрактами НАТО; порядок отримання сертифікатів допуску для персоналу підприємств, які виконують контракти з НАТО; умови міжнародного транспортування класифікованих матеріалів за контрактами з НАТО; порядок виконання міжнародних візитів за

контрактами з НАТО; порядок залучення позаштатного персоналу для виконання проектів та програм НАТО.

Індустріальна безпека на додаток до стандартних засобів безпеки вимагає створення національних органів індустріальної безпеки, класифікації контрактів з організаціями НАТО, сертифікації обладнання з приводу безпеки, введення спеціальних заходів для забезпечення безпеки транспортування класифікованих матеріалів та міжнародних візитів [141]. Велика роль при цьому надається національним органам безпеки (NOS). NOS керує організаціями з виробництва та логістики НАТО (NPLOs) і промисловими проектами НАТО з питань безпеки.

3.9. Норми поводження з несекретною інформацією НАТО.

Документ **C-M(2002)60 (NATO/Unclassified)** встановлює норми поводження з несекретною інформацією НАТО. Відповідно до політики безпеки НАТО така інформація поділяється на дві категорії:

а) «НАТО/некласифікована, але чутлива» (NATO/Unclassifiedbut sensitive);

б) «НАТО/некласифікована» (NATO/Unclassified).

Згідно з Документом **C-M(2002)60**, до інформації NATO/ Unclassified but Sensitive належить інформація, що не має ступеня секретності, але має адміністративний гриф або гриф обмеження розповсюдження. Така інформація НАТО може використовуватися лише для офіційних цілей і лише особами,
органами або організаціями, яким вона необхідна для офіційних цілей НАТО.

Адміністративні грифи можуть застосовуватися до документів тільки автором, де це необхідно, з метою ідентифікації типу інформації, що міститься в ньому, та зазначення потреби в обмеженому доступі. Адміністративні грифи НАТО може мати така інформація:

Комерційна: Commercial	Інформація про комерційну власність, наприклад, отримані внаслідок поставки продукції за контрактами НАТО.
Управлінська: Management	Інформація щодо управління та планування, яка має вплив на інтереси НАТО.
Медична: Medical	Інформація щодо медичних доповідей або пов'язані з цим матеріали, які стосуються персоналу та підрозділів НАТО.
Особиста: Personal	Інформація, яка належить фізичній особі або яка їй адресована і рішення щодо оприлюднення якої належить цій фізичній особі.
Щодо штату: Staff	Інформація, що містить посилання на визначеного або невизначеного співробітника(ів).

Також можуть застосовуватися адміністративні грифи обмеження розповсюдження, що обмежують передачу інформації лише до визначеної групи.

Згідно з Документом C-M(2002)60, до інформації «НАТО/некласифікована» (NATO/Unclassified) належить інформація, яку можна оприлюднювати. Така інформація не повинна мати жодних грифів.

4.Завдання лабораторної роботи.

4.1. Дати аналіз і описати основні принципи забезпечення безпеки інформації в країнаї НаТО і ЄС.

4.2. Проаналізувати і описати базові стандарти НАТО із захисту інформації з обмеженим доступом.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Терміни: «національна безпека», «інформаційна безпека» та «організаційно-правові основи інформаційної безпеки» (в Україні).
2. Наведіть короткий зміст документа С-М (2000) 49.
3. Охарактеризуйте базові принципи, які адекватно відображають сутність захисту інформації, та ступені секретності інформації в країнах НАТО та ЄС.
4. Наведіть основні принципи, що забезпечують високий рівень інформаційної безпеки в країнах НАТО та ЄС і розкрийте їх зміст.
5. Охарактеризуйте сутність політики безпеки та види інформації в докуметах країн НАТО і ЄС.
6. Принципи захисту інформації та інституційного документа С-М(2002)49.
7. Ступені секретност інформації в країнах НАТО і ЄС.
8. На які директиви опирається документ С-М (2000) 49?
9. Які види стандартів в системі «STANAG» Ви знаєте? Наведіть їх характеристику.
10. Охарактеризуйте структуру Органів безпеки НАТО.
11. Наведіть структуру документа С-М (2000) 49.
12. Навеведіть задачі, заходи і зони фізичної безпеки в НАТО.
13. Охарактеризуйте заходи і процедури безпеки персоналу в НАТО.
14. Яким чином проводиться розповсюдження інформації в країнах НАТО?
15. Охарактеризуйте заходи і засоби забезпечення промислової та індустріальної безпеки в країнах НАТО та ЄС.
16. Наведіть правила поводження з несекретною інформацією вкраїнах НАТО.

Тема – 2. ВИВЧЕННЯ МІЖНАРОДНОГО СТАНДАРТУ З ОЦІНЮВАННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ISO/IEC 15408)

1.Мета роботи.

Ознайомлення з європейською методикою оцінювання безпеки інформаційних технологій, яка включає процес розроблення і кваліфакаційного аналізу продуктів інформаційних технологій, структуру профілю захисту та завдання з безпеки.

2.Необхідна література:

Стандарти з оцінювання безпеки інформаційних технологій (різних версій типу ISO/IEC 18045:2005 Information technology – Security technigues – Methodology for security

М.В. Грайворонський, О.М. Новіков Безпека інформаційно-комунікаційних систем. Підручник. Видавнича група BHV, К. 2009. С.179-189.

3.Основні теоретичні відомості.

3.1.Завдання стандарта ISO/IEC 15408.

Основними завданнями з розроблення цього стандарта були: уніфікація національних стандартів у сфері оцінювання безпеки ІТ; підвищення рівня довіри до оцінювання безпеки ІТ; скорочення витрат на оцінювання рівня безпеки Інформаційних технологій (ІТ) на основі взаємного визнання сертифікатів.

3.2.Зміст «Загальних критеріїв», структура стандарта ISO/IEC 15408, область застосування «Загальних критеріїв» та неоліки стандарта.

Документ ISO/IEC 15408 має такі основні розділи: вступ і загальна модель, функціональні вимоги безпеки та вимоги до забезпечення безпеки.

У документі розглянуто основні аспекти безпеки — забезпечення конфіденційності, цілісності та доступності інформації або, інакше кажучи, захист від несанкціонованого доступу, модифікації чи втрати доступу до інформації під час реалізації загроз.

Під керівництвом ISO було також розроблено нормативно-методичну документацію, як додаток до стандарту, що містить: вказівки щодо розроблення профілів захисту та визначення завдань захисту; процедури реєстрації профілів захисту; загальну методологію оцінювання безпеки ІТ.

Стандарт ISO/IEC 15408, призначений для оцінювання безпеки продуктів ІТ. «Загальні критерії» можуть стати у пригоді: розробникам об'єктів оцінювання; експертам з оцінювання об'єктів; користувачам об'єкта оцінювання.

Об'єктом оцінювання ми називатимемо продукт або систему ІТ, яка має ресурси, що можна використовувати для оброблення та зберігання інформації. Об'єктами оцінювання можуть бути операційні системи, інформаційні системи, обчислювальні мережі, прикладні програми тощо.

Недоліки стандарту

У «Загальних критеріях» не приділено достатньо уваги адміністративним заходам і технічним засобам безпеки, стандарт не містить критеріїв оцінювання криптографічних методів захисту інформації та рекомендацій щодо самих методик оцінювання. Певною мірою це було враховано лише в нормативно-методичній документації, виданій на підтримку стандарту.

3.3. Базові поняття

Згідно з концепцією «Загальних критеріїв» вимоги до безпеки об'єкта оцінювання поділяють на дві категорії:

- функціональні вимоги, тобто вимоги до тих функцій об'єкта оцінювання, що відповідають за безпеку ІТ-продукту;
- вимоги адекватності (або гарантованості) описують такі властивості об'єкта оцінювання, які гарантують ефективність і коректність реалізації необхідних засобів його безпеки.

У стандарті використано єдину ***термінологію*** для визначення функціональних вимог і вимог гарантованості:

- ***клас*** — найбільш загальна група вимог безпеки;
- ***сімейство*** — член класу, який визначає групу вимог, що

забезпечують виконання певної частини цілей безпеки;

- ***компонент*** — член сімейства, який визначає мінімальний набір вимог безпеки для включення до структур, визначених у «Загальних критеріях»;
- ***елемент*** — неподільна складова компонента.

Така ієрархія дає змогу під час ідентифікації загроз безпеці виділити з їх загальних характеристик окремі компоненти і елементи.

У «Загальних критеріях» визначено також сукупність структур, які поєднують компоненти вимог безпеки. До таких структур належать:

- ***пакет*** (Package) — проміжна комбінація компонентів, яка містить набір вимог, що відповідають визначеному піднабору цілей безпеки (пакет призначений для багаторазового використання);
- ***-рівень гарантованості оцінювання*** (Evaluation Assurance Level) — визначений пакет вимог гарантованості;
- ***-профіль захисту*** (Protection Profile) — набір вимог, що складається з компонентів або пакетів функціональних вимог і одного з рівнів гарантованості (профіль захисту специфікує сукупність вимог, необхідних і достатніх для досягнення заданих цілей безпеки);
- ***завдання з безпеки*** (Security Target) — набір вимог, визначених одним із профілів захисту або сформульованих явно.

3.4. Розроблення ІТ-продукту та його кваліфікаційний аналіз

Стандарт ISO/IES 15408 використовують на різних етапах життєвого циклу ІТ-продукту, насамперед під час його розроблення та кваліфікаційного аналізу. На рис.1 показано застосування «Загальних критеріїв» на різних етапах життєвого циклу ІТ-продукту.

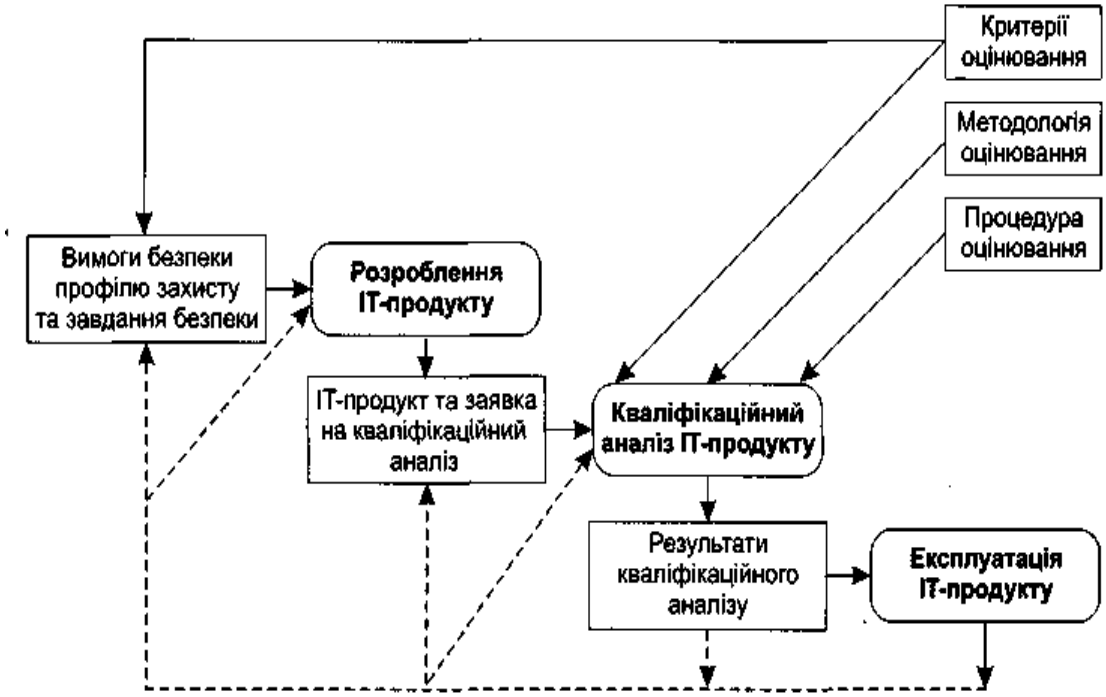

Рис.1. Використання «Загальних критеріїв» на етапах існування ІТ-продукту.

Піддаючи ІТ-продукт кваліфікаційному аналізу, окрім «Загальних критеріїв» слід використовувати документ «Загальна методологія», де подано перелік дій, які необхідно виконати під час оцінювання.

Основні принципи, на яких ґрунтується «Загальна методологія»: результати оцінювання є об'єктивними і не залежними від суб'єктивного бачення експерта, дії експерта, який використовує одну й ту саму методику оцінювання, приводять до несуперечливих результатів, дії експерта забезпечують точне технічне оцінювання.

Процес оцінювання об'єкта здійснюється у три етапи: отримання вихідних даних для оцінювання, проведення оцінювання, оформлення результатів оцінювання.

Це етапи узагальненої моделі процесу оцінювання, де передбачено взаємодію таких учасників:

- ***заявник***—ініціатор та замовник оцінювання (він є відповідальним за надання експерту-оцінювачу необхідних відомостей);

♦- ***розробник***—демонструє об'єкт оцінювання і відповідає за надання відомостей;

♦ ***експерт-оцінюва*** - приймає відомості від розробника або безпосередньо від заявника, здійснює оцінювання об'єкта та надає його результати відповідному органу;

♦ ***орган оцінюванн***—організовує, підтримує і контролює процес оцінювання (на основі отриманих від експертів-оцінювачів результатів оцінювання надає сертифікати і випускає звіти про сертифікацію).

Оцінювання може бути здійсненим із використанням різних методів і прийомів; це залежить від заявлених вимог довіри та предмета оцінювання.

Формування критеріїв оцінювання об'єкта виконується шляхом висування ***якісних вимог*** до функціональних механізмів гарантування безпеки та визначення ***кількісних показників*** для проведення оцінювання.

Серед матеріалів, які використовують для проведення кваліфікаційного аналізу, можна виділити:

♦ завдання з безпеки, де описано функції захисту ІТ-продукту та вимоги безпеки, що відповідають вимогам профілю захисту, на реалізацію якого претендує продукт;

♦ відомості про можливості ІТ-продукту, подані його розробником;

♦ ІТ-продукт;

♦ додаткові відомості, отримані після проведення різних експертиз.

3.5. Етапи здійснення кваліфікаційного аналізу.

Кваліфікаційний аналіз ІТ-продукту здійснюють у кілька етапів.

1. Аналіз профілю захисту на його повноту, несуперечність, можливість реалізації та використання як набору вимог до продукту, що аналізують.
2. Аналіз завдання з безпеки на його відповідність вимогам профілю захисту, а також на повноту, несуперечність, можливість реалізації та використання як опису ІТ-продукту.

3.Аналіз ІТ-продукту на його відповідність завданню з безпеки.

3.6. Профіль захисту.

1.**Вступ**. У вступі подано інформацію, необхідну для пошуку профілю в бібліотеці профілів (ідентифікатор) і огляд змісту.

2.**Опис об'єкта оцінювання**. Тут подано стислу характеристику об'єкта оцінювання, його функціональне призначення, принцип роботи, методи використання тощо. Ця інформація не підлягає аналізу і сертифікації.

3.**Середовище експлуатації**.

У цьому розділі подано опис усіх аспектів функціонування об'єкта оцінювання, пов'язаних з безпекою.

3.1.**Загрози безпеці**.

Опис загроз безпеці, яким має протистояти захист. Для кожної загрози вказуються джерело, метод впливу, об'єкт.

3.2.**Політика безпеки**.

Тут подано визначення і пояснення правил політики безпеки..

3.3.**Умови експлуатації**.

Тут надається вичерпна характеристика середовища експлуатації в контексті безпеки.

4.**Задачі захисту**.

Йдеться про потреби користувачів протидіяти зазначеним загрозам безпеці та (або) реалізовувати політику безпеки.

До задач захисту належать такі.

4.1.**Задачі захисту, які вирішує сам ІТ-продукт**.

4.2.**Інші задачі захисту**.

5.**Вимоги безпеки**.

Йдеться про вимоги безпеки, які має задовольняти ІТ-продукт для вирішення задач захисту. До цих вимог належать такі.

5.1.**Функціональні вимоги**.

Лише типові вимоги, передбачені у відповідних розділах «Загальних критеріїв», які можуть зобов'язувати чи забороняти використовувати конкретні методи та засоби.

5.2.**Вимоги адекватності**. Це також лише типові вимоги.

5.3.**Вимоги до середовища експлуатації**.

Це необов'язковий розділ. Функціональні вимоги та (або) вимоги адекватності до середовища експлуатації.

6.**Додаткові відомості**.

Цей розділ не є обов'язковим. У ньому можуть бути викладені, наприклад, вказівки щодо застосування профілю захисту.

7.**Обґрунтування**.

Тут наведено доводи того, що профіль захисту містить повну і зв'язну множину вимог, а ІТ-продукт, який їх задовольняє, здатний ефективно протистояти загрозам безпеці середовища експлуатації.

Зокрема, наведено таке.

3.7. Завдання з безпеки

Нижче наведено інформацію про структуру завдання з безпеки та зміст основних розділів.

1.**Вступ.** У цьому розділі йдеться про призначення завдання з безпеки, а також подано інформацію, необхідну для ідентифікації завдання. Розділ містить таке.

1.1.**Ідентифікатор.** Унікальне ім'я, яке використовують для пошуку й ідентифікації завдання з безпеки і відповідного йому ІТ-продукту.

1.2.**Огляд змісту**. Докладна анотація завдання з безпеки, ознайомившись із якою споживач зможе дізнатися, чи здатний ІТ-продукт вирішити його задачі.

1.3.**Заявка на відповідність «Загальним критеріям».**

Опис усіх властивостей ІТ-продукту, що підлягають кваліфікаційному аналізу на основі «Загальних критеріїв».

2.**Опис ІТ-продукту**. Стислий опис продукту.

3.**Середовище експлуатації.** Уміст підрозділів цього розділу відповідає вмісту аналогічних підрозділів зі структури профілю захисту.

3.1.Загрози безпеці.

3.2.Політика безпеки.

3.3.Умови експлуатації.

4.**Задачі захисту.** Цей розділ також збігається з однойменним розділом профілю захисту.

4.1.Задачі захисту, що вирішує ІТ-продукт.

4.2.Інші задачі захисту.

5.**Вимоги безпеки.** Тут наведено вимоги безпеки, якими керувався розробник ІТ-продукту, що дає йому змогу заявляти про успішне вирішення задач захисту.

6.**Загальні специфікації ІТ-продукту**.

Відображення реалізації ІТ-продуктом вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту. Серед цих специфікацій виокремлюють такі.

6.1.**Специфікації функцій захисту.** Опис функціональних можливостей засобів захисту ІТ-продукту, заявлених розробником як такі, що реалізують вимоги безпеки. Форма подання специфікацій сприяє визначенню відповідності між функціями захисту і вимогами безпеки.

6.2.**Специфікації рівня адекватності.** Визначається заявлений рівень адекватності захисту ІТ-продукту та його відповідність вимогам адекватності через подання параметрів технології проектування і створення ІТ-продукту.

7.**Заявка на відповідність профілю захисту.** Цей розділ також є необов'язковим. Завдання з безпеки претендує на задоволення вимог одного чи кількох профілів захисту, для кожного з яких розділ буде містити таку інформацію.

8.**Обґрунтування.** Тут доводиться, що завдання з безпеки містить повну і зв'язну множину вимог, що ІТ-продукт, який їх реалізує, здатний ефективно протистояти загрозам безпеці середовища експлуатації і що загальні специфікації функцій захисту відповідають вимогам безпеки.

4.Завдання лабораторної роботи.

4.1. Виконати аналіз змісту стандарта **ISO/IEC 15408** і описати методику оцінювання безпеки інформаційних технологій.

4.2. Ознайомитись з новою версією стандарта **ISO/IEC 15408**: 2008 на основі третьої версії «Загальних критерів»або з діючою версією - **ISO/IEC 18045:2005 [ISO/IEC 18045:2005 Information technology – Security technigues – Methodology for security evalution].**

КОНТРОЛЬНІ ЗАПИТАННЯ

1.Назвіть основні завдання стандарту ISO/IEC 15408.
2.З яких розділів складається і для чого призначений стандарт ISO/IEC 15408?
3.Які недоліки присутні цьому стандарту?
4.Охарактеризуйте базові поняття стандарта ISO/IEC 15408.
5.Охарактеризуйте застосування «Загальних критеріїв» на різних етапах життєвого циклу ІТ – продукту.
6.Що включає процес оцінюванняоб`єкта за «Загальною методологією»?
7.Які є категорії вимог (згідно з ISO/IEC 15408) до безпеки об'єкта оцінювання?
8.Які матеріали використовуються для проведення кваліфікаційного аналізу?
9.Охарактеризуйте основні етапи здійснення кваліфікаційного аналізу.
10.Що таке профіль захисту? Яку він має структуру?
11.Чим структура завдання з безпеки відрізняється від структури профілю захисту?
12.У чому полягають переваги ієрархії вимог виду клас-сімейство-компонент-елемент?

ТЕМА-3. ВИВЧЕННЯ ОРГАНІЗАЦІЙНОЇ РОБОТИ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

1.Мета роботи.

Ознайомлення з роботою служби захисту інформації в автоматизованих системах Підприємства.

2.Необхідна література.

М.В. Грайворонський, О.М. Новіков Безпека інформаційно-комунікаційних систем. Підручник. Видавнича група BHV, К. 2009. С.553-583.

М.М. Зацеркляний, О.Ф. Мельников Основи економічної безпеки. Навчальний посібник. –К.: КНТ, 2007. – С. 122-145.

3.Основні теоретичні відомості.

3.1.Супроводження комплексної системи захисту інформації. Положення про службу захисту інформації в автоматизованій системі.

Організацію робіт із впровадження та підтримки роботоздатності Комплексної системи захисту інформації (КСЗІ) виконує служба захисту інформації (СЗІ). Діяльність такої служби регламентує положення про службу захисту інформації, що має назву «Типове положення про службу захисту інформації в автоматизованій системі».

У загальному випадку документ «Типове положення про службу захисту інформації в автоматизованій системі» складається 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 розпис і структура служби захисту інформації.

♦ Організація робіт служби захисту інформації.
♦ Фінансування служби захисту інформації.

3.1. Загальні положення

Це нормативний документ організації чи АС, який визначає завдання, функції, штатну структуру служби захисту інформації, повноваження, статус та відповідальність її співробітників, взаємодію з іншими підрозділами та із зовнішніми організаціями.

Метою створення СЗІ є організаційне забезпечення завдань управління КСЗІ в АС та здійснення контролю за її функціонуванням. СЗІ має визначати вимоги захисту інформації в АС, проектувати, розробляти та модернізувати КСЗІ, експлуатувати, обслуговувати та підтримувати її дієздатність, а також контролювати рівень захищеності інформації в АС.

Служба захисту інформації здійснює діяльність відповідно до «Плану захисту інформації в автоматизованій системі», календарних, перспективних та інших планів робіт, затверджених керівником організації.

СЗІ взаємодіє з іншими підрозділами організації (РСО, службою безпеки, підрозділом ТЗІ тощо), а також із державними органами, установами та організаціями, що займаються питаннями захисту інформації.

3.2. Завдання та функції служби захисту інформації

Основні завдання СЗІ:

- захист законних прав щодо безпеки інформації в організації, окремих її структурних підрозділах, персоналу під час обміну інформацією між собою та із зовнішніми вітчизняними та закордонними організаціями;
- дослідження технології оброблення інформації в АС задля виявлення ймовірних каналів її витоку та інших загроз безпеці інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;
- організація та координація заходів, пов'язаних із захистом інформації в АС, потребу в захисті якої визначає її власник або чинне законодавство, та підтримка належного рівня

захищеності інформації, ресурсів і технологій;
- розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими має підтримуватися певний рівень захисту інформації в АС;
- організація заходів із створення і використання КСЗІ на всіх етапах життєвого циклу АС;
- організація професійної підготовки і підвищення кваліфікації персоналу та користувачів АС з питань захисту інформації;
- формування у персоналу і користувачів думки щодо необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються питань захисту інформації;
- забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації в АС та проведення контрольних перевірок їх виконання.
-виконання певних функцій під час створення КСЗІ;
-виконання відповідних функцій під час експлуатації КСЗІ;
-організація навчання персоналу з питань забезпечення захисту інформації.

Під час ***створення КСЗІ*** служба захисту інформації виконує наступні функції:
♦ визначення даних, які підлягають захисту під час їх оброблення, та інших об'єктів захисту в АС, класифікація інформації за вимогами до її конфіденційності або значущості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення) інформації та її використання;
♦ розроблення та коригування моделі загроз, моделі захисту інформації та політики безпеки інформації в АС;
♦ визначення і формування вимог до КСЗІ;
♦ організація і координація заходів із проектування та розроблення КСЗІ, безпосередня участь у проектуванні КСЗІ;
♦ підготовка технічних пропозицій, рекомендацій щодо

запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;

- ♦ організація заходів і участь у випробуваннях КСЗІ, проведенні її експертизи;
- ♦ добирання організацій — виконавців робіт зі створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення заходів із 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 тощо);
- ♦ участь у розробленні нормативних документів, чинних у межах організації та АС, які встановлюють дисциплінарну відповідальність за порушення вимог із безпеки інформації та встановлених правил експлуатації КСЗІ;
- ♦ участь у розробленні нормативних документів, чинних у межах організації та АС, які встановлюють правила доступу користувачів до ресурсів АС, визначають порядок, норми, правила із захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій тощо).

Під час ***експлуатації КСЗІ*** служба захисту інформації виконує наступні функції:

♦ організація процесу управління КСЗІ;

♦ розслідування випадків порушення політики безпеки, небезпечних та непередбачуваних подій, аналізування подій, що спричинили ці порушення, здійснення супроводу банку даних таких подій;

♦ проведення заходів у разі виявлення спроб НСД до ресурсів АС, порушення правил експлуатації засобів захисту інформації чи інших дестабілізуючих факторів;

♦ забезпечення контролю цілісності засобів захисту інформації та можливості швидкого реагування на їх вихід із ладу чи порушення режимів функціонування;

♦ організація управління доступом до ресурсів АС (розподіл між користувачами необхідних реквізитів захисту інформації: паролів, привілеїв, ключів тощо);
♦ супроводження й актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об'єктів, ідентифікатори користувачів тощо);
♦ спостереження (реєстрація й 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 із модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій АС або КСЗІ;
♦ участь у заходах із модернізації АС: узгодженні пропозицій щодо введення до складу АС нових компонентів, функціональних завдань і режимів оброблення інформації, заміни засобів оброблення інформації тощо;
♦ забезпечення супроводження й актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ та їх зберігання і тестування;
♦ аналітичне оцінювання поточного стану безпеки інформації в АС (прогнозування виникнення нових загроз та їх урахування в моделі загроз, визначення потреби в її коригуванні, аналіз відповідності технології оброблення інформації та реалізованої політики безпеки поточній моделі загроз тощо);
♦ інформування власників інформації про технічні можливості захисту інформації в АС і встановлені для персоналу і користувачів АС типові правила;
♦ втручання у 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 із захисту інформації;
♦ аналізування відомостей про технічні засоби захисту

інформації нового покоління, обґрунтування пропозицій із придбання таких засобів для організації;

♦ здійснення контролю за виконанням персоналом і користувачами АС вимог, норм, правил, інструкцій із захисту інформації відповідно до визначеної політики безпеки інформації, зокрема за дотриманням режиму секретності у разі оброблення в АС інформації, що становить державну таємницю;

♦ здійснення контролю за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

♦ розроблення та реалізація спільно з РСО (підрозділом ТЗІ, службою безпеки) комплексних заходів із забезпечення безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами (нарад, переговорів тощо), а також здійснення їхнього технічного та інформаційного забезпечення.

Організацію навчання персоналу забезпеченню захисту інформації здійснюють таким чином:

♦ розробляють плани навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу АС;

♦ розробляють спеціальні програми навчання з урахуванням особливостей технології оброблення інформації в організації (АС), необхідного рівня її захищеності тощо;

♦ організовують та проводять навчання користувачів і персоналу АС правилам роботи з КСЗІ, захищеними технологіями та ресурсами;

♦ узгоджують навчальні плани і плани з підвищення кваліфікації з державними органами, навчальними закладами та іншими організаціями;

♦ забезпечують навчальний процес необхідною матеріальною базою, посібниками, нормативно-правовими актами, нормативними документами, методичною літературою тощо.

3.3. Права й обов'язки служби захисту інформації

Служба захисту інформації має право:

- ♦ здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (АС) щодо виконання ним вимог нормативно-правових актів і нормативних документів із захисту інформації;
- ♦ пропонувати керівництву організації призупиняти процес оброблення інформації, забороняти його, змінювати режими оброблення у разі виявлення порушень політики безпеки або виникнення реальної загрози безпеці;
- ♦ складати і надавати керівництву організації акти виявлених порушень політики безпеки, готувати рекомендації щодо їх усунення;
- ♦ здійснювати службові розслідування у разі виявлення порушень;
- ♦ отримувати доступ до документів структурних підрозділів організації (АС), необхідних для оцінювання ефективності вжитих заходів із захисту інформації та підготовки пропозицій щодо подальшого їх удосконалення;
- ♦ вносити пропозиції щодо залучення на договірній основі до проведення заходів із захисту інформації інших організацій, які мають ліцензії на відповідний рід діяльності;
- ♦ вносити пропозиції щодо забезпечення АС (КСЗІ) технічними і програмними'" та засобами захисту інформації чи іншою спеціальною технікою, яка дозволена для використання в Україні з метою забезпечення захисту інформації;
- ♦ вносити на розгляд керівництва організації пропозиції щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;
- ♦ узгоджувати умови додавання до АС нових компонентів та надавати керівництву пропозиції щодо заборони їх використання, якщо вони порушують прийняту політику безпеки або знижують рівень захищеності ресурсів АС;

- надавати висновки щодо питань, які належать до компетенції СЗІ, насамперед щодо технологій, доступ до яких обмежено, та проектів, що потребують технічної підтримки з боку співробітників СЗІ;
- надавати керівництву організації пропозиції щодо узгодження планів і регламенту відвідування АС сторонніми особами;
- здійснювати інші дії, права на виконання яких надано СЗІ відповідно до специфіки та особливостей діяльності організації (АС).

Служба захисту інформації повинна виконуватинаступні функції:

- забезпечувати якісне виконання організаційно-технічних заходів із захисту інформації в АС;
- вчасно і в повному обсязі надавати користувачам і персоналу АС інформацію про змінення у сфері захисту інформації;
- перевіряти відповідність прийнятих в АС (організації) правил, інструкцій щодо оброблення інформації, здійснювати контроль за виконанням цих вимог;
- здійснювати контрольні перевірки стану захищеності інформації в АС;
- забезпечувати конфіденційність заходів із монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в АС (організації);
- сприяти і, за потреби, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в АС;
- сприяти створенню і дотриманню умов зберігання інформації, отриманої організацією на договірних, контрактних або інших основах від організацій-партнерів, постачальників, клієнтів та приватних осіб;
- періодично, не рідше ніж раз на місяць, надавати керівництву організації звіт про стан захищеності інформації в АС і про дотримання користувачами та персоналом АС встановленого порядку і правил захисту

інформації;
- ♦ негайно повідомляти керівництво АС (організації) про виявлені атаки та викритих порушників.

Відповідальність за діяльність СЗІ покладено на її керівника, який зобов'язаний:

- ♦ організовувати заходи із захисту інформації в АС, забезпечувати ефективність захисту інформації відповідно до діючих нормативно-правових актів;
- ♦ забезпечувати своєчасне розроблення і виконання «Плану захисту інформації в автоматизованій системі»;
- ♦ контролювати виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у Положенні, посадових інструкціях, а також планових заходів із захисту інформації, затверджених керівником організації;
- ♦ координувати плани діяльності підрозділів та служб АС (організації) з питань захисту інформації;
- ♦ організовувати навчання співробітників, користувачів, персоналу АС щодо питань захисту інформації;
- ♦ виконувати особисто правила внутрішнього трудового розпорядку, встановленого режиму, правила охорони праці та протипожежної охорони, а також контролювати виконання всіх цих правил співробітниками СЗІ.

Співробітники СЗІ відповідають за:

- ♦ дотримання вимог нормативних документів, де визначено порядок організації робіт із захисту інформації, інформаційних ресурсів та технологій;
- ♦ повноту та якість розроблення і впровадження організаційно-технічних заходів із захисту інформації в АС, точність та достовірність отриманих результатів і висновків з питань компетенції СЗІ;
- ♦ дотримання термінів проведення контролюючих, інспекційних, перевірочних та інших заходів із оцінювання стану захищеності інформації в АС, долучених до плану робіт СЗІ;

- ♦ якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;
- ♦ виконання інших дій в АС.

3.4. Взаємодія служби захисту інформації з іншими підрозділами та із зовнішніми організаціями

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

Заходи із захисту інформації в автоматизованих системах СЗІ має узгоджувати із заходами охоронної та режимно-секретної діяльності інших підрозділів організації.

СЗІ взаємодіє з такими структурами: РСО організації, підрозділом ТЗІ організації; адміністрацією АС та іншими підрозділами організації, діяльність яких пов'язана із захистом інформації або її автоматизованим обробленням; 4 службою безпеки організації; зовнішніми організаціями; підрозділами служб безпеки іноземних фірм, їхніми представниками; іншими суб'єктами діяльності у сфері захисту інформації.

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

3.5. Штатний розклад і структура служби захисту інформації

СЗІ є штатним підрозділом організації, безпосередньо підпорядкованим керівнику організації або його заступнику, який відповідає за забезпечення безпеки інформації, або є структурною (штатною або позаштатною) одиницею підрозділу ТЗІ організації. Штатність чи позаштатність СЗІ встановлюють на підставі рішення, прийнятого на загальних зборах акціонерів або керівництвом організації.

Структуру СЗІ, її склад і чисельність визначають на підставі фактичних потреб АС із забезпечення вимог політики безпеки інформації, їх затверджує керівництво

організації. Чисельність і склад СЗІ мають бути достатніми для виконання всіх завдань із захисту інформації в АС.

Для ефективного функціонування й управління захистом інформації в АС СЗІ має штатний розклад, який містить перелік функціональних обов'язків усіх співробітників, необхідних вимог до рівня їхніх знань і навичок.

Безпосереднє керівництво роботою СЗІ здійснює її керівник; якщо СЗІ є структурною одиницею підрозділу ТЗІ (служби безпеки організації) — керівник цього підрозділу. Керівника СЗІ призначає та звільняє з посади керівництво організації, узгодивши свої дії з особами, відповідальними за безпеку інформації.

Функціональні обов'язки співробітників визначено переліком і характером завдань, які покладає на СЗІ керівництво АС (організації).

До складу **СЗІ** можуть входити різні за фахом спеціалісти (групи спеціалістів, підрозділи тощо): спеціалісти з питань захисту інформації від її витоку технічними каналами; спеціалісти з питань захисту каналів зв'язку і комутаційного обладнання, настроювання і управління активним мережним обладнанням; спеціалісти з питань адміністрування засобів захисту, управління базами даних; спеціалісти з питань захищених технологій обробки інформації.

За посадами співробітників СЗІ поділяють на такі категорії робочого персоналу: керівник СЗІ, адміністратори захисту АРМ (безпеки баз даних, безпеки системи тощо); спеціалісти служби захисту.

Змінити структуру СЗІ можна лише на підставі рішення, прийнятого на загальних зборах акціонерів або керівництвом організації та затвердженого наказом (розпорядженням) керівника.

3.6. Організація заходів служби захисту інформації та їх фінансування

СЗІ здійснює свою роботу з реалізації основних організаційно-технічних заходів зі створення та забезпечення

функціонування КСЗІ згідно з планами робіт. Основою для розроблення планів заходів є «План захисту інформації в АС».

Плани містять ***заходи наступних типів***: разові (виконуються один раз, другий раз — лише після повного перегляду прийнятих рішень із захисту інформації); такі, що виконуються постійно; такі, що виконуються періодично (із заданим проміжком часу); що виконуються за потреби.

Основні види планів заходів СЗІ:

- ♦ календарний план заходів із проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації КСЗІ тощо;
- ♦ план заходів із оперативного реагування на непередбачувані ситуації (зокрема, надзвичайні та аварійні) та відновлення функціонування АС;
- ♦ поточний план заходів (на місяць, квартал, рік);
- ♦ перспективний план розвитку та вдосконалення діяльності СЗІ з питань захисту інформації (до 5 років);
- ♦ план дій із забезпечення безпеки інформації окремих заходів (проведення нарад, укладання договорів, угод тощо);
- ♦ бізнес-план створення і функціонування СЗІ.

Плани заходів складає керівник СЗІ після обговорення на виробничій нараді організаційно-технічних питань і затверджує керівник організації або підрозділу, куди входить СЗІ.

Реорганізацію або ліквідацію СЗІ можна здійснити на підставі рішення, прийнятого на загальних зборах акціонерів або керівництвом організації. Реорганізаційну або ліквідаційну процедуру здійснює відповідна комісія, яка створюється за наказом керівника організації.

З метою забезпечення конфіденційності робіт, які виконують співробітники СЗІ, вони, влаштовуючись на роботу, дають письмові зобов'язання не розголошувати відомості, які становлять службову, комерційну або іншу таємницю.

СЗІ фінансують за рахунок: коштів, виділених організацією на утримання органів управління; прибутку організації (АС) та інших коштів за рішенням, прийнятим керівництвом організації або на загальних зборах акціонерів; коштів, отриманих за виконання СЗІ договірних робіт та надання послуг; інших джерел фінансування, не заборонених законодавством.

4.Рекомендації щодо структури та змісту Плану захисту інформації в автоматизованій системі

Діяльність СЗІ спирається на План захисту інформації. ***План захисту інформації в АС*** (далі План захисту) — це набір документів, згідно з якими організують захист інформації протягом життєвого циклу АС.

План захисту інформації в АС розробляють на основі проведеного аналізу технології оброблення інформації та наявних ризиків, а також сформульованої політики безпеки інформації. План захисту визначає і документально скріплює об'єкт захисту інформації в АС, основні завдання захисту, загальні правила оброблення інформації в АС, мету створення та функціонування КСЗІ, заходи із захисту інформації. План захисту має фіксувати на певний проміжок часу склад АС, технологію оброблення інформації, склад комплексу засобів захисту інформації, перелік необхідної документації тощо.

План захисту містить такі пункти: завдання захисту інформації в АС; класифікація інформації, що обробляють в АС; опис компонентів АС та технології оброблення інформації; загрози для інформації в АС; політика безпеки інформації в АС; система документів із забезпечення захисту інформації в АС.

4.1. Завдання захисту інформації в АС

До завдань захисту інформації в АС належать такі:

- ефективне знешкодження загроз ресурсам АС шляхом комплексного впровадження правових, морально-етичних,

фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

- ♦ забезпечення визначених політикою безпеки властивостей інформації під час створення та експлуатації АС;
- ♦ своєчасне виявлення та знешкодження загроз ресурсам АС, причин та умов виникнення порушень функціонування АС та її розвитку;
- ♦ створення механізму та умов оперативного реагування на загрози безпеці інформації, інші прояви негативних тенденцій у функціонуванні АС;
- ♦ управління засобами захисту інформації, доступом користувачів до ресурсів АС, контроль за їхньою роботою з боку персоналу СЗІ, оперативне сповіщення про спроби НСД до ресурсів АС;
- ♦ реєстрація, збирання, зберігання, оброблення даних про всі події в системі, пов'язані з безпекою інформації;
- ♦ створення умов для максимально можливого відшкодування та локалізації збитків, що завдають неправомірні (несанкціоновані) дії фізичних та юридичних осіб, вплив зовнішнього середовища та інші чинники, а також зменшення негативного впливу наслідків порушення безпеки на функціонування АС.

Політика безпеки, яку реалізує КСЗІ для захисту інформації від потенційних внутрішніх та зовнішніх загроз, ***має охоплювати такі об'єкти захисту:***

- ♦ відомості, що належать до інформації з обмеженим доступом (ІзОД) або інші види інформації, що підлягають захисту, яку обробляють в АС;
- ♦ інформаційні масиви і бази даних, програмне забезпечення та інші інформаційні ресурси;
- ♦ обладнання АС та інші матеріальні ресурси, зокрема технічні засоби та системи, що не задіяні в обробленні ІзОД, але розташовані в контрольованій зоні, носії інформації, процеси і технології її оброблення. До технічних областей, в яких необхідно захищати інформаційне та програмне забезпечення, належать робоча

станція, комунікаційні канали та комутаційне обладнання, сервери, засоби для створення твердих копій даних, накопичува-чі інформації;

- ♦ засоби і системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;
- ♦ користувачів (персонал) АС, власників інформації та АС, а також їхні права.

Безпеку інформації в АС забезпечують шляхом:

- ♦ організації та впровадження системи допуску співробітників до інформації, яка потребує захисту;
- ♦ організації обліку, зберігання, обігу інформації, яка потребує захисту, та її носіїв;
- ♦ організації та координації робіт із захисту інформації, яка обробляється та передається засобами АС;
- ♦ здійснення контролю за забезпеченням захисту інформації, яку обробляють засоби АС, і за збереженням конфіденційних документів (носіїв).

4.2. Класифікація інформації, що обробляють в АС

Класифікація інформації дає змогу її власнику (розпоряднику) або власнику автоматизованої системи визначити методи і способи захисту даних кожного окремого типу. Всі дані в АС класифікують за режимом доступу, правовим режимом, а також за типом їх подання.

За режимом доступу інформацію в АС поділяють на ***відкриту*** та ***з обмеженим доступом.***

Відкриту інформацію, у свою чергу, поділяють на таку, що не потребує захисту або захист якої забезпечувати недоцільно, і таку, що потрібно захищати.

Інформація з обмеженим доступом — це важлива для особи, організації, суспільства чи держави інформація, порушення конфіденційності якої може призвести до моральних чи матеріальних збитків.

За правовим режимом інформацію з обмеженим доступом поділяють на таємну та конфіденційну.

До ***таємної інформації*** належить така, що містить відомості, які становлять державну чи іншу, передбачену законом, таємницю.

Правила доступу до конфіденційної інформації, володіти, користуватися чи розпоряджатися якою можуть окремі фізичні, юридичні особи або держава, встановлює її власник. Якщо інформація становить велику цінність для її власника, то втрата або передавання такої інформації іншим особам може завдати організації (власнику) великої шкоди. З метою встановлення ПРД до конфіденційної інформації її слід класифікувати, поділивши на категорії з урахуванням цінності даних.

Для встановлення правил взаємодії активних і пасивних об'єктів автоматизованої системи інформацію класифікують за типом її подання в АС (для кожної з визначених категорій встановлюють типи пасивних об'єктів комп'ютерної системи, якими вона може бути представлена).

4.3. Компоненти АС і технології оброблення інформації

Перш ніж складати опис компонентів АС, необхідно провести їх інвентаризацію.

Інвентаризації підлягають такі об'єкти:

- обладнання — комп'ютерні системи та їх компоненти (процесори, монітори, термінали, робочі станції тощо), периферійні пристрої;
- програмне забезпечення;
- дані тимчасового і постійного;
- персонал і користувачі АС.

Окрім компонентів АС до опису долучають технології оброблення інформації, що потребує захисту, тобто способи і методи застосування засобів обчислювальної техніки під час здійснення функцій збирання, зберігання, оброблення, передавання і використання даних або алгоритмів окремих процедур. Опис (системи) може бути неформальним або формальним.

Для відображення інформаційної взаємодії між основними компонентами АС (завданнями, об'єктами)

доцільно розробити схему інформаційних потоків, указавши для кожного елемента схеми категорію інформації та визначені політикою безпеки рівні доступу до неї.

4.4. Загрози інформації і політика безпеки інформації в АС

Щоб можна було проводити аналіз ризиків і формувати вимоги до КСЗІ, необхідно розробити модель загроз інформації та модель порушника. Ці роботи здійснюють на підготовчому етапі створення КСЗІ за результатами обстеження АС. Модель загроз і модель порушника слід документально оформити та долучити до Плану захисту.

Політику безпеки інформації також розробляють на підготовчому етапі створення КСЗІ в АС, документально оформлюють і долучають до Плану захисту. Політику безпеки покладено в основу створення КСЗІ.

4.5. Календарний план робіт із захисту інформації в АС

На основі Плану захисту інформації в АС складають календарний план робіт із реалізації заходів захисту інформації в АС, який містить наступні пункти: організаційні заходи; контрольно-правові заходи; профілактичні заходи; інженерно-технічні заходи; робота з кадрами.

Організаційні заходи із захисту інформації — це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне виконання завдань захисту інформації шляхом регламентації діяльності персоналу і функціонування засобів (систем) забезпечення інформаційної діяльності та засобів забезпечення захисту інформації.

До плану можуть бути долучені такі заходи:

- розроблення документів з різних напрямів захисту інформації в АС;
- внесення змін і доповнень до чинних в АС документів з урахуванням змінен-ня умов (обставин);
- розроблення й впровадження нових організаційних заходів із захисту інформації;
- обґрунтування необхідності застосування та впровадження

нових засобів захисту інформації;

- ♦ координація робіт з іншими підрозділами організації або зовнішніми організаціями на всіх етапах життєвого циклу АС;
- ♦ перегляд результатів виконання затверджених заходів і робіт із захисту інформації.

До контрольно-правових заходів, зокрема, належать такі:

- ♦ контроль за виконанням персоналом (користувачами) вимог відповідних інструкцій, розпоряджень і наказів;
- ♦ контроль за виконанням заходів, розроблених за результатами попередніх перевірок;
- ♦ контроль за станом зберігання й використання носіїв інформації на робочихмісцях.

Профілактичні заходи спрямовані на формування у персоналу (користувачів) мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт тощо, а також на формування відповідного морально-етичного стану в колективі.

До ***інженерно-технічних*** належать 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 розміщено засоби оброблення інформації, зокрема й під час капітального будівництва тощо.

До ***плану робіт із кадрами*** потрібно долучати заходи з добирання й навчання персоналу (користувачів) встановленим правилам безпеки інформації, новим методам захисту інформації, а також із підвищення їхньої кваліфікації. Навчання можна здійснювати власними силами, із залученням спеціалістів із зовнішніх організацій або в інших організаціях. Навчання здійснюють згідно з програмою, затвердженою керівництвом організації (АС). Навчальні програми мають містити теоретичний і практичний курси.

Таким чином, супроводження діючих систем захисту інформації в інформаційно-комунікаційних системах є важливою складовою забезпечення безпеки інформації. Цей процес регламентовано вітчизняними нормативними документами та стандартами. Використання міжнародних стандартів сприяє підвищенню якості реалізації систем захисту. В Україні діє нормативний документ НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»,який регулює всі аспекти створення та діяльності структурного підрозділу або окремих осіб, відповідальних за безпеку інформації, що обробляється в інформаційній системі. У додатку до «Типового положення про службу захисту інформації в автоматизованій системі» наведено вимоги щодо розроблення й оформлення керівних документів, на основі яких вживають заходів із захисту інформації. Ці документи утворюють так званий План захисту як окремі його розділи або як пакет окремих документів.

5.Завдання лабораторної роботи.

5.1. Ознайомитись з «Типовим положенням про службу захисту інформації в автоматизованій системі» та рекомендаціями щодо структури і змісту Плану захисту інформації в автоматизованій системі.

5.2. На основі «Типового положення про службу захисту інформації в автоматизованій системі», розробити зразки положень про службу захисту інформації в автоматизованій системі науково-дослідного фізико-технічного інституту (ВАРІАНТ-А) або комерційного банку (ВАРІАНТ-Б).

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Яким основним документом керується у своїй діяльності служба захисту інформації?
2. З яких розділів складається «Типове положення…….».
3. Охарактеризуйте статус служби захисту інформації (СЗІ).
4. Якою є мета створення СЗІ?
5. Якими є основні завдання СЗІ?
6. Які функції виконує СЗІ під час створення КСЗІ?
7. Які функції виконує СЗІ під час експлуатації КСЗІ?
8. Охарактеризуйте процедуру навчання персоналу забезпеченню захисту інформації.
9. Які права має СЗІ?
10. Які функції виконує СЗІ?
11. В чому полягають основні обов`язки керівника СЗІ?
12. За що відповідають співробітники СЗІ?
13. З якими структурами взаємодіє СЗІ?
14. Охарактеризуйте штатний розклад і структуру типової СЗІ.
15. Які спеціалісти можуть входити до складу СЗІ?
16. Які типи заходів входять до плану захисту інформації в автоматизованій системі?
17. За рахунок яких коштів фінансується СЗІ?
18. Дайте визначення і загальну характеристику «Плану захисту інформації в АС».
19. Які основні пункти містить план захисту інформації в АС?
20. В чому полягають завдання захисту інформації в АС?
21. Які об`єкти охоплені плітикою безпеки КСЗІ?
22. Якими шляхами забезпечується безпека інформації в АС?
23. Які об`єкти АС підлягають інвентаризації?
24. З яких пунктів складається календарний план робіт із реалізації заходів захисту інформації в АС?
25. Які заходи можна віднести до контрольно-правових в календарному плані робіт із захисту інформації?
26. Які додаткові заходи можуть бути долучені до календарного плану захисту інформації в АС?

ТЕМА-4. УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

1.Мета роботи.

Ознайомлення з основними правилами управління безпекою роботи інформаційно-комунікаційних систем

2.Необхідна література:

М.В. Грайворонський, О.М. Новіков Безпека інформаційно-комунікаційних систем. Підручник. Видавнича група BHV, К. 2009. С.553-583.

ISO/IEC 27002 «Інформаційні технології — Методики безпеки — Практичні правила управління інформаційною безпекою»

3.Основні теоретичні відомості. Стандарт: ISO/IEC 27002 «Інформаційні технології — Методики безпеки — Практичні правила управління безпекою інформації»

3.1. Загальні відомості про стандарт

Для врегулювання комплексу питань із захисту інформації в організаціях крім зазначеної вище групи документів використовують інші, зокрема міжнародні стандарти. Найбільш поширеними міжнародними стандартами, з цього питання є стандарт BSI «Настанова із захисту інформаційних технологій для базового рівня захищеності» та новітні стандарти серії ISO/IEC 27000 зі створення, розвитку та підтримки системи менеджменту інформаційної безпеки (СМІБ).

Розглянемо докладніше міжнародний стандарт ISO/IEC 27002 «Інформаційні технології — Методики безпеки — Практичні правила управління безпекою інформації». Цей стандарт вирізняється з-поміж інших високим рівнем абстрактності та лаконізмом, тому його можуть успішно застосовувати висококваліфіковані та досвідчені фахівці з інформаційної безпеки.

3.1. Структура й основний зміст стандарту

Документ складається з передмови, вступу та 15 розділів. Розділи мають номери з 1-го по 15-й, вступ

позначено як 0-й розділ. Далі наведено перелік усіх розділів і подано їх стислий зміст.

0.Вступ.
1.Сфера застосування.
2.Терміни та визначення.
3.Структура стандарту.
4.Оцінювання й оброблення ризиків.
5.Політика безпеки.
6.Організація забезпечення безпеки інформації.
7.Управляння ресурсами.
8.Безпека персоналу.
9.Фізична безпека і безпека середовища.
10.Управління комунікаціями й операціями.
11.Управління доступом.
12.Придбання, розроблення та супроводження інформаційних систем.
13.Управління інцидентами безпеки.
14.Управління безперебійністю бізнесу.
15.Дотримання вимог.

У вступі розгнуто наступні питання:

- що таке безпека інформації?;
- чому необхідна безпека інформації?;
- як затвердити вимоги до безпеки?;
- визначення ризиків безпеки;
- вибір засобів управління.
- відправна точка безпеки інформації.
- критичні фактори успіху.
- розроблення власних рекомендацій із захисту інформації організації.

Розглянемо окремі положення вступу більш детально.

У перших двох підрозділах вступу наведено визначення поняття безпеки інформації, її мету, завдання, мотивацію необхідності захисту".

Підрозділ «Як затвердити вимоги до безпеки» визначає три головних джерела вимог до системи безпеки організації:

- специфічні ризики порушення безпеки, які загрожують ресурсам організації і для яких оцінюють уразливість та ймовірність її виникнення, а також потенційний вплив;
- набір правових і договірних вимог, які мають виконувати організація, її торговельні партнери, підрядники та постачальники послуг;
- набір специфічних принципів, цілей та вимог до оброблення інформації, розроблений організацією.

У підрозділі «Визначення ризиків безпеки» відзначають важливість відповідності між цінністю інформаційних ресурсів організації та витратами на систему їх захисту. При цьому слід ураховувати рівень ризику та збитки, яких може бути завдано організації внаслідок порушення безпеки інформації. Ризики слід визначати періодично задля урахування будь-яких змінень, що впливають на безпеку.

Після визначення вимог до безпеки та ризиків необхідно обрати й упровадити прийнятні засоби управління для зниження ризиків. Питання добирання таких засобів обговорено у підрозділі «Вибір засобів управління».

У підрозділі «Відправна точка безпеки інформації» зазначено, що використання *багатьох* із засобів управління можна вважати відправною *точкою для* впровадження системи безпеки інформації. Засоби управління, які є суттєвими для організації з позиції законодавства, можуть здійснювати захист: конфіденційності даних і особистої інформації, документів організації і прав інтелектуальної власності.

До заходів і засобів, які вважають необхідними для створення системи безпеки інформації, належать:

- ♦ створення документа про політику безпеки інформації;
- ♦ розподіл обов'язків із забезпечення безпеки інформації;
- ♦ навчання й підготовка персоналу з питань дотримання режиму безпеки інформації;
- ♦ технічне управління вразливостями;
- ♦ підтримка безперебійної роботи;

♦ управління інцидентами безпеки інформації.

У підрозділі «Критичні фактори успіху» визначено фактори, критичні для успішного впровадження безпеки інформації в організації:

♦ політика, цілі й діяльність із захисту інформації, що відображають цілі бізнесу;
♦ підхід і структурна основа для впровадження, супроводження і вдосконалення захисту інформації;
♦ суттєва підтримка і зобов'язання всіх рівнів керівництва;
♦ розуміння вимог безпеки інформації, визначення ризиків і управління ними;
♦ надання рекомендацій з політики й стандартів безпеки інформації всім керівникам, співробітникам та іншим сторонам;
♦ фінансування заходів з управління безпекою інформації;
♦ забезпечення належних знань, навчання й освіти персоналу;
♦ управління інцидентами інформаційної безпеки;
♦ упровадження системи показників, призначеної для оцінювання ефективності управління безпекою інформації.

У підрозділі «Розроблення власних рекомендацій із захисту інформації організації» визначено, що кожна організація може мати власний набір вимог, проблем, пріоритетів і керівних принципів безпеки інформації. Якщо організація має документи із власними рекомендаціями щодо захисту інформації, то вони мають містити посилання на цей стандарт задля встановлення взаємозв'язків між відповідними розділами.

Сфера застосування (розділ 1). Уданому розділі подано інформацію щодо призначення стандарту. Стандарт містить рекомендації та загальні принципи з ініціювання, впровадження, супроводження й удосконалення управління безпекою інформації в організації. Стандарт можна використовувати як практичну рекомендацію з розроблення власних стандартів організацій та ефективної практики управління безпекою інформації, а також для сприяння

встановленню довірчих відносин під час взаємодії між організаціями.

Терміни та визначення (розділ2). Розділ містить інформацію про основні терміни та визначення безпеки інформації. Зокрема, термін «безпека інформації» тут визначено як збереження властивостей інформації, на кшталт конфіденційності, цілісності та доступності.

Структура стандарту (розділ 3). У розділі описано структуру стандарту (його підрозділи було названо вище). Вимоги стандарту викладено в його розділах 4-15. У них сформульовано 39 цілей управління, досягнення яких забезпечує захист інформаційних ресурсів від загроз їх конфіденційності, цілісності та доступності. Опис цілей керування фактично містить специфікації функціональних вимог до архітектури управління безпекою інформації організації. Для кожної із цілей керування названо засоби керування, що можуть бути застосовані для досягнення загальної мети керування.

Оцінювання й оброблення ризиків (розділ 4). У розділі показано відповідність між цінністю інформаційних ресурсів організації та витратами на систему захисту інформації. Для визначення витрат на систему захисту мають бути враховані рівень ризику та збитки, яких може бути завдано організації. Ризики мають зумовлювати належні пріоритети і дії керівництва щодо управління безпекою інформації та впровадження засобів, обраних для захисту від цих ризиків.

Під час визначення ризиків слід застосовувати системний підхід до обчислення величини ризиків і порівняння обчислених ризиків із критеріями їх значущості. Для кожного з ризиків слід прийняти рішення щодо його оброблення (усунення чи зниження). Можливі варіанти оброблення ризиків:

♦ застосування прийнятних засобів управління для зниження ризиків;

- ♦ свідоме прийняття ризиків за умови забезпечення їх відповідності політиці організації й критеріям прийняття ризиків;
- ♦ усунення ризиків шляхом заборони дій, що можуть викликати ці ризики;
- ♦ перекладання ризиків на інші сторони, наприклад на страховиків або постачальників.

Для оброблення ризиків необхідно обрати й впровадити засоби управління з урахуванням: вимог та обмежень національного й міжнародного законодавства, цілей організації, робочих вимог і обмежень, вартості впровадження засобів управління ризиками.

Політика безпеки (розділ 5). Роз'яснення цілей і здійснення всебічної підтримки захисту інформації шляхом чіткого формулювання політики безпеки — обов'язок вищого керівництва. Наявність документа про політику безпеки інформації є однією з цілей керівництва. У розділі рекомендовано наступний зміст цього документа:

- ♦ визначення захисту інформації, його головні цілі та сфера застосування, значення захисту інформації як механізму, що дає змогу використовувати її колективно;
- ♦ викладення позиції керівництва з питань реалізації цілей і принципів захисту інформації;
- ♦ тлумачення конкретних варіантів політики безпеки, принципів, стандартів і вимог до її дотримання, зокрема: виконання правових і договірних вимог, вимоги щодо навчання персоналу правил безпеки, політика попередження і виявлення вірусів,
- ♦ політика забезпечення безперебійної роботи організації;
- ♦ визначення загальних і конкретних обов'язків із забезпечення режиму безпеки інформації;
- ♦ роз'яснення процедури сповіщення про події, які можуть впливати на безпеку інформації.

Окремий підрозділ присвячено порядку ревізії політики безпеки. Ревізію необхідно проводити періодично із запланованим інтервалом, а також у випадку суттєвих змінень, що можуть впливати на політику безпеки.

Організація забезпечення безпеки інформації (розділ 6). У цьому розділі визначено дві цілі управління в таких підрозділах.

1. Інфраструктура безпеки інформації організації.

   Для забезпечення захисту інформації слід створити відповідну структуру управління в організації. Необхідно проводити регулярні наради керівництва, присвячені коригуванню політики безпеки інформації, розподілу обов'язків із забезпечення захисту та координації дій, спрямованих на підтримку режиму безпеки. За потреби для консультацій слід залучити фахівців відповідного рівня. З метою обміну досвідом необхідно встановлювати контакти з фахівцями інших організацій. Слід всебічно впроваджувати комплексний підхід до розв'язання проблем безпеки інформації.

2. Питання безпеки доступу сторонніх організацій.

   Під час взаємодії із сторонніми організаціями, зокрема, у разі застосування їхніх продуктів або послуг, необхідно унеможливити компрометацію безпеки інформації. Для цього слід уживати узгоджених з іншими організаціями заходів із підтримки режиму безпеки. Потрібно провести аналіз ризиків і визначити вимоги до засобів управління, що знижують ці ризики. Відповідні засоби та заходи управління мають бути зафіксовані в угоді зі сторонньою організацією.

Управління ресурсами (розділ 7). Організація має чітко усвідомлювати, якими інформаційними ресурсами вона володіє, і керувати їхньою безпекою належним чином. У двох підрозділах цього розділу визначено цілі такого управління.

1. **Відповідальність за ресурси.** Усі ресурси повинні бути враховані та мати своїх відповідальних. Обладнання та інший інвентар, що можуть впливати на інформаційні ресурси (апаратне та програмне забезпечення, дані, документація, носії інформації, допоміжні пристрої і системи на кшталт кондиціонерів повітря та джерел безперебійного живлення) також необхідно належним чином супроводжувати.

2. **Класифікація інформації**.

З метою визначення пріоритетів щодо захисту інформації необхідно провести її класифікацію за категоріями значущості. Таку систему класифікації слід використовувати задля визначення рівнів захисту інформації та сповіщення користувачів щодо необхідності спеціального поводження з нею.

Безпека персоналу (розділ 8). Розділ присвячено питанням відображення завдань безпеки в посадових інструкціях, а також під час надання інформаційних ресурсів, навчання користувачів, реагування на події, що містять загрозу безпеці тощо. Головна мета заходів безпеки, відображених у посадових інструкціях, полягає у зменшенні ризиків на кшталт помилок персоналу, крадіжок, шахрайства чи незаконного використання ресурсів. Основним механізмом управління є надання персоналу певних прав доступу до ресурсів. Цей розділ складається з таких трьох підрозділів.

1. **Наймання персоналу**. Усі пов'язані з безпекою питання слід враховувати ще під час наймання персоналу на роботу. Вимоги щодо безпеки потрібно висвітлювати в описі вакансій, обговорювати в ході інтерв'ю, долучати до посадових інструкцій і угод, а також контролювати їх протягом усього перебування співробітника в організації. Керівництво організації має переконатися, що в посадових інструкціях враховано всі вимоги безпеки, які виконуватиме працівник, перебуваючи на своїй посаді. Осіб, яких наймають на роботу, передусім тих, хто працюватиме з конфіденційною інформацією, потрібно належним чином перевіряти. Увесь персонал організації та користувачі інформаційних ресурсів зі сторонніх організацій мають підписати зобов'язання про нерозголошення конфіденційної інформації.
2. **Виконання посадових обов'язків**. Навчання персоналу — одне з важливих питань управління безпекою інформації в організації. Метою навчання є надання користувачам інформаційних ресурсів відомостей про загрози порушення

режиму безпеки інформації, а також необхідних навичок із забезпечення режиму нормального функціонування системи безпеки цієї організації. Усі співробітники та підрядники мають бути ознайомлені з процедурою оповіщення про інциденти різного типу (порушення безпеки, загрози тощо), які можуть вплинути на безпеку ресурсів організації. В організації має бути впроваджена процедура поширення дисциплінарних стягнень на співробітників, які порушують режим безпеки.

3. **Звільнення з посади чи її змінення**.Особливу увагу слід приділяти питанням безпеки під час звільнення співробітників або їх переведення на інші посади. Слід контролювати повернення співробітником ресурсів, які йому було надано, а також скасування прав доступу.

Фізична безпека і безпека середовища (розділ 9). У розділі розглянуто заходи зі створення та адміністрування зон безпеки і контрольованих периметрів, а також заходи щодо здійснення контролю за доступом до приміщень. Велику увагу приділено заходам із захисту обладнання організації. Тут ідеться про те, що вимоги до фізичного захисту можна змінювати залежно від масштабів і структури інформаційних сервісів, а також з урахуванням уразливості та критичності виробничих процесів, які підтримуються. Визначено також дві цілі управління в таких підрозділах.

1. **Зони безпеки**. Мета заходів зі створення та адміністрування зон безпеки — запобігти несанкціонованому доступу до інформаційних ресурсів, їх пошкодженню і створенню перешкод у їх роботі. Для цього організують концентричні зони із засобами фізичного контролю доступу між ними. Інформаційні системи, які підтримують критично важливі чи вразливі сервіси, мають бути розташовані в зонах із належним контролем доступу. Для зменшення ризику несанкціонованого доступу чи ушкодження паперової , документації та носіїв інформації пропонується встановлювати чіткі правила використання робочого місця.

2. **Безпека обладнання**. Мета заходів з організації захисту обладнання — запобігати втраті, ушкодженню, компрометації ресурсів і збоям у роботі організації. Слід забезпечити захист критичного обладнання інформаційних систем від навмисного чи випадкового фізичного пошкодження, пожежі, затоплення, крадіжки, перегрівання, раптових вимкнень електричного живлення тощо. Розглянуто питання захисту допоміжного обладнання (системи електричного живлення чи структурованої кабельної системи) та необхідності безпечної утилізації обладнання і носіїв інформації.

Управління комунікаціями й операціями (розділ 10).

Розділ присвячено організаційним заходам адміністрування комп'ютерних систем і мереж задля забезпечення їх коректної та надійної роботи. Вимоги до безпечного адміністрування комп'ютерних систем і мереж можна змінювати залежно від масштабу та структури інформаційних сервісів, а також від ступеня вразливості та критичності виробничих процесів, які ця система підтримує. У підрозділах цього розділу визначено десять цілей управління.

1. **Робочі процедури та відповідальність**. Для безпечного адміністрування комп'ютерних систем і мереж необхідно визначити обов'язки персоналу та відповідні процедури. Ці заходи слід підтвердити відповідними робочими інструкціями та операційними процедурами реагування на події для зменшення ризику недбалого чи несанкціонованого використання систем. За потреби слід застосовувати принцип розмежування обов'язків, наприклад відокремити доступ до засобів розроблення та робочих програм.
2. **Управління послугами сторонніх підрядників**. Залучення стороннього підрядника може призвести до порушення режиму безпеки. Необхідно заздалегідь виявити такий ризик і долучити до контракту належні захисні заходи, узгоджені з підрядником.
3. **Планування й приймання систем**. Планування систем і їх

приймання дають змогу звести ризики відмов систем до мінімуму. Для забезпечення досяжності ресурсів систем та їх належного навантаження ці ресурси необхідно попередньо спланувати і підготувати. З цією метою слід спрогнозувати потенційні вимоги до параметрів обладнання, задати критерії приймання нових систем і провести відповідні випробування. Слід також спланувати заходи щодо ймовірного переходу на аварійний режим роботи та постійно контролювати процес внесення змін у робочі системи.

4. **Захист від шкідливого та мобільного коду**. Дієвим заходом із забезпечення цілісності даних і програм є захист від шкідливого програмного забезпечення. Для попередження і виявлення випадків проникнення шкідливого програмного забезпечення потрібно впроваджувати належні застережливі заходи. Окремо розглянуто заходи захисту для мобільного коду, що підтримується зв'язувальним програмовим забезпеченням.

5. **Резервне копіювання**. Заходи із обслуговування систем дають змогу підтримувати цілісність і доступність сервісів. Необхідно визначити щоденні процедури резервного копіювання даних, реєстрації подій і збоїв, а також процедури спостереження за середовищем функціонування обладнання.

6. **Управління безпекою мережі**. Заходи з адміністрування мережі забезпечують захист інформації, яка циркулює в мережі, а також в інфраструктурі її підтримки. Управління безпекою комп'ютерних мереж, окремі сегменти яких розміщено поза межами організації, потребує особливої уваги. Необхідно вжити спеціальних заходів захисту до конфіденційних даних, які передаються через мережі загального доступу. Тут розглянуто такі сервіси безпеки, як приватні мережі та міжмережне екранування.

7. **Захист носіїв даних**. Слід визначити порядок безпечної роботи з комп'ютерними носіями даних, паперовими документами, системною документацію для забезпечення фізичного захисту під час їх використання, перевезення,

зберігання. Потрібно ретельно контролювати процедури знищення носіїв даних.

8. **Інформаційний обмін**. З метою запобігання втратам, модифікаціям і несанкціонованому використанню інформації обмін даними і програмами між організаціями необхідно контролювати, наприклад, впровадженням політик і процедур, а також укладанням відповідних угод. Особливу увагу слід приділити захисту електронного обміну повідомленнями, електронної пошти, документообігу.

9. **Сервіси електронної комерції**. Застосування систем електронної комерції потребує ретельної уваги до питань безпеки. Слід також захищати цілісність і доступність інформації, яку публікують у комп'ютерній мережі.

10. **Моніторинг**. Слід впроваджувати реєстрацію пов'язаних із безпекою подій і здійснювати їх аудит, вести протокол збоїв, забезпечити сповіщення вповноважених адміністраторів про події задля виявлення неавторизованого доступу. Необхідними допоміжними заходами є убезпечення журналів реєстрації та синхронізація системних годинників.

Управління доступом (розділ 11). Даний розділ присвячено розгляду питань із здійснення контролю за логічним доступом до комп'ютерних систем і даних, що дає змогу запобігати несанкціонованому доступу. У розділі сформульовано сім цілей управління у таких підрозділах.

1. **Вимоги бізнесу щодо контролю доступу**. Вимоги організації щодо управління доступом користувачів до інформаційних ресурсів повинні бути прозоро задокументовані у політиці управління доступом, що має враховувати правила поширення інформації та розмежування доступу. Можна застосовувати профілі доступу, що відповідають посадам співробітників.
2. **Управління доступом користувачів**. Надання прав доступу користувачам слід здійснювати з дотриманням певних формальних процедур реєстрації й адміністрування користувачів — від початкової реєстрації нових користувачів до видалення облікових записів користувачів, з обов'язковою періодичною ревізією прав і повноважень

користувачів. Особливу увагу слід приділяти процедурі надання привілейованих прав доступу користувачам, які надають їм можливість обійти засоби системного контролю.

3. **Відповідальність користувачів**. Користувачі мають добре знати свої обов'язки із забезпечення ефективного контролю доступу, насамперед щодо використання паролів та захисту обладнання від доступу сторонніх осіб.
4. **Управління доступом до мережі**. Управління доступом до мережі забезпечує захист систем, об'єднаних у таку мережу. Контроль слід забезпечувати як усередині корпоративної мережі, так і під час обміну між організаціями. До числа засобів контролю необхідно долучити механізми автентифікації віддалених користувачів та обладнання. Інформаційні мережні сервіси, користувачі та системи мають бути розподілені на логічні мережні домени з урахуванням встановленої в організації політики доступу.
5. **Управління доступом до операційних систем**. Одним з важливих заходів управління безпекою інформації є управління доступом до комп'ютерів, здійснюваним на рівні операційних систем. Доступ слід надавати лише зареєстрованим користувачам. У випадку багатокористувацьких систем слід ідентифікувати та перевіряти справжність (автентичність) користувачів наданням їм унікальних ідентифікаторів і паролів доступу. Необхідно фіксувати випадки успішного та невдалого доступу до систем і використання привілеїв, підтримувати систему управління паролями, яка забезпечує добирання надійних паролів, за потреби обмежувати час підключення користувачів.
6. **Управління доступом до прикладних програм та інформації**. Управління доступом до прикладних програм дає змогу запобігати несанкціонованому доступу до прикладних систем і даних. Доступ до них слід надавати лише зареєстрованим користувачам згідно з визначеною політикою управління доступом. Особливо чутливі

прикладні сервіси потребують виділених (ізольованих) платформ та додаткових засобів контролю.

7. **Використання мобільних обчислень і віддалених робітників**. Мають існувати формальні політики, які б врегульовували безпечне використання портативних ПК, комунікаторів, мобільних телефонів, а також безпечний режим взаємодії з віддаленими робітниками.

Придбання, розроблення та супроводження інформаційних систем (розділ 12). Цей розділ присвячено питанням урахування вимог безпеки в рамках загального плану робіт із створення інформаційної системи. Для цього вимоги до безпеки систем необхідно визначати та узгоджувати під час розроблення специфікацій, розроблення, придбання, тестування, введення в дію й супроводження інформаційно-комунікаційних систем. Цей розділ містить шість підрозділів.

1. **Вимоги безпеки інформаційних систем**. На стадії розроблення вимог до системи слід проаналізувати і повністю ідентифікувати вимоги безпеки. Придбане програмне забезпечення має пройти тестування безпеки.
2. **Коректність прикладних систем**. Під час проектування прикладних систем слід вбудувати в них засоби управління безпекою, зокрема засоби реєстрації подій в контрольному журналі. Необхідно контролювати захищеність файлів прикладних систем. Користувачі прикладної системи та їх розробники зобов'язані підтримувати цілісність цих програм.
3. **Криптографічний захист**. Слід визначити політику застосування засобів криптографічного захисту, яка може містити ролі та відповідальність, цифровий підпис, неможливість відмови, управління ключами та цифровими сертифікатами тощо.
4. **Безпека системних файлів**. Слід контролювати доступ до системних файлів: виконуваних програм, вихідного коду, тестових даних.
5. **Безпека процесів розроблення і супроводження**. Середовище розробки і робоче середовище слід жорстко

контролювати. Необхідно здійснювати аналіз усіх змін, які планується внести у системи, задля гарантування того, що ними не буде порушено безпеку середовища розробки та робочого середовища. За потреби слід проводити перевірку ймовірних витоків інформації через приховані канали чи внаслідок дії «троянського коня». Додаткові заходи управління і моніторингу пропонують задіяти у разі залученні до розроблення зовнішніх виконавців.

6. **Управління вразливостями**. Управління вразливостями систем і прикладних програм здійснюється шляхом моніторингу оприлюдненої інформації про виявлені вразливості, оцінювання пов'язаних із ними ризиків і усунення вразливостей шляхом оновлень і виправлень програм.

Управління інцидентами безпеки інформації (розділ 13). Даний розділ присвячено питанням виявлення подій, що впливають на безпеку інформації, та слабких місць у системі безпеки задля гарантування можливості вживати своєчасних заходів протидії. Розділ містить такі два підрозділи.

1. **Повідомлення про інциденти безпеки інформації та слабкі місця**. Впровадження формального порядку сповіщень про різні типи подій і виявлених слабких місць, що можуть впливати на безпеку ресурсів організації. Усі співробітники та контрагенти мають бути поінформовані про такий порядок і зобов'язані невідкладно повідомляти про будь-які події та слабкі місця.
2. **Управління інцидентами безпеки інформації та удосконаленнями**. Впровадження порядку ефективного невідкладного оброблення подій і слабких місць. Забезпечення відповідності юридичним вимогам потребує наявності певної доказової бази.

Управління безперебійністю бізнесу (розділ 14). Розділ присвячено питанням планування безперебійної роботи організації. З метою убереження критично важливих виробничих процесів від наслідків великих аварій і катастроф необхідно розробляти плани забезпечення можливості

безперебійної роботи організації на ці випадки. Процес планування безперебійної роботи організації має містити заходи з ідентифікації та зменшення ризиків, ліквідації наслідків від реалізації загроз і швидкого поновлення виробничих процесів і сервісів.

Дотримання вимог (розділ 15). У розділі наведено рекомендації щодо дотримання юридичних вимог, а також вимог політик і стандартів безпеки. Він складається з трьох підрозділів.

1. **Дотримання юридичних вимог**. Необхідно забезпечити дотримання юридичних вимог з метою виключення порушень будь-яких законів, статутних, нормативних або договірних зобов'язань і будь-яких вимог безпеки, зокрема вимог із захисту фінансової інформації, обмежень у використанні криптографічного захисту, правил збирання доказів під час розслідування інцидентів тощо.
2. **Дотримання вимог політик і стандартів безпеки**. Стан безпеки інформаційних систем необхідно регулярно перевіряти. Ці перевірки слід проводити виходячи з відповідної політики безпеки, а технічні платформи й інформаційні системи необхідно перевіряти на відповідність прийнятим стандартам забезпечення безпеки. Необхідно мінімізувати втручання в процес тестування систем на рівень інформаційної безпеки. Для цього необхідно мати засоби контролю та захисту засобів тестування і робочих систем під час їх роботи.
3. **Застосування аудита інформаційних систем.** Слід упровадити засоби управління із захисту діючих систем та інструментів аудита під час проведення аудита інформаційних систем. Також необхідно здійснювати захист цілісності з метою запобігання неправомірному використанню інструментів аудита.

Інші стандарти серії ISO 27000 містять правила, рекомендації та специфікації у сфері безпеки інформації для створення, розвитку й підтримки системи менеджменту інформаційної безпеки (СМІБ), яку ще називають системою управління інформаційною безпекою (СУІБ) (Information

Security Management System, ISMS). СМІБ є складовою загальної системи менеджменту, що базується на підході бізнес-ризиків під час створення, впровадження, функціонування, моніторингу, аналізу, підтримки й удосконалення інформаційної безпеки.

Окрім розглянутого вище ISO/IEC 27002 у цій серії оприлюднено ще такі стандарти:

ISO/IEC 27001:2005 «Інформаційні технології — Методики безпеки — Системи менеджменту інформаційної безпеки — Вимоги» — стандарт, за яким організація може бути сертифікована;

ISO/IEC 27005:2008 «Інформаційні технології — Методики безпеки — Управління ризиками інформаційної безпеки» — стандарт, що надає рекомендації з управління безпекою інформації на основі підходу управління ризиками;

ISO/IEC 27006:2007 «Інформаційні технології — Методики безпеки — Вимоги до організацій, що проводять аудит і сертифікацію систем менеджменту інформаційної безпеки» — настанова з акредитації сертифікаційних організацій.

Активно розробляють також наступні стандарти: **ISO/IEC 27000** — глосарій для стандартів СМІБ, **ISO/IEC 27003** — новий довідник із створення СМІБ, **ISO/IEC 27004** — новий стандарт для вимірювань у галузі інформаційної безпеки, **ISO/IEC 27007** - стандарт з аудита СМІБ, **ISO/IEC 27011** — настанова з телекомунікацій у СМІБ та **ISO/IEC 27033** — стандарт із безпеки комп'ютерних мереж.

Контрольні запитання

1. Охарактеризуйте структуру і основний зміст стандарта **ISO/IEC 15408**.
2. Які питання безпеки інформації висвітлено у вступі до стандарта?
3. В чому полягають необхідні заходи і засоби для створення системи безпеки інформації за стандартом **ISO/IEC 15408?**
4. Сфера застосування статдарта **ISO/IEC 15408**.
5. Оцінювання і оброблення ризиків. Можливі варіанти оброблення ризиків.

6. Охарактеризуйте політику безпеки згідно стандарта **ISO/IEC 15408**.
7. Що пропонує стандарт **ISO/IEC 15408** в сфері організаційного забезпечення безпеки інформації?
8. Охарактеризуйте зміст розділу з управління ресурсами.
9. Які питання в стандарті розглянуто в розрізі безпеки персоналу?
10. Фізична безпека і безпека обладнання (зони безпеки, безпека обладнання).
11. Управління комунікаціями і операціями.
12. Управління доступом.
13. Придбання, розроблення і супровід інформаційних систем.
14. Управління інцидентами безпеки інформації.
15. Дотримання вимог.

4. Завдання лабораторної роботи.

4.1. Виконати аналіз змісту стандарта і описати методику оцінювання безпеки інформаційних технологій.

4.2. Ознайомитись з новою версією стандарта **ISO/IEC 15408**: 2008 на основі третьої версії «Загальних критерів»або з діючою версією - **ISO/IEC 18045:2005 [ISO/IEC 18045:2005 Information technology – Security technigues – Methodology for security evalution].**

5. **Питання модульного контролю (№1)**

1. Основні проблеми інформаційної безпеки і базові принципи створення системи безпеки інформації в Україні.
2. Що складає загрози інформаційній безпеці України (зовнішньополітична сфера, сфери державної і військової безпеки України та інформаційна сфера)?
3. Сформулюйте основні концептуальні питання інформаційної безпеки України.
4. Концепція технічного захисту інформації в Україні та технічний захист інформації. Причини виникнення загроз безпеці інформації.
5. В чому полягають основні функції організаційних структур системи технічного захисту інформації (ТЗІ)?
6. Дайте характеристику першочерговим заходам щодо реалізації державної політики, які визначає концепція ТЗІ в Україні.
7. Дайте коротку характеристику документів С-М(55) 15 та С-М (2000) 49. Наведіть базові принципи, які адекватно відображають сутність захисту інформації в країнах НАТО та ЄС.
8. Охарактеризуйте ступені секретності інформації в країнах НАТО та ЄС.
9. Що є предметом розгляду національного законодавства країн-кандидатів на членство в НАТО при встановленні ступеня відповідпальності за неправомірне розкриття конфіденційної інформації?
10. Порядок робіт зі створення комп`ютерної системи захисту інформації. Структура комплексно системи захисту інформації (КСЗІ).
11. Етапи робіт зі створення КСЗІ та основні чинники, які слід враховувати в моделі загроз безпеці інформації.
12. Що повинна визначати модель порушника?
13. Наведіть загальні відомості про політику безпеки та охарактеризуйте основні принципи, покладені в основу політики безпеки.
14. Основні кроки розроблення політики безпеки.
15. Організація виконання відновлювальних робіт і забезпечення неперервного функціонування АС.
16. Загальні вимоги до розроблення технічного завдання (ТЗ) на створення комплексної системи захисту інформації. Основні етапи розроблення ТЗ.
17. Наведіть зміст основних підрозділів ТЗ.

18. Охарактеризуйте зміст робіт при введенні в дію КСЗІ.
19. Загальні вимоги до кваліфікаційного аналізу засобів і систем захисту інформації.
20. Хто приймає участь в державній експертизі? Охарактеризуйте планг здійснення експертизи.
21. Охарактеризуйте процедуру і основні етапи сертифікації засобів технічного зазисту інформації.
22. Основні етапи проведення технічного захисту інформації в Україні. Шляхи здійснення загроз безпеці інформаці Ваим відомі ?
23. Охарактеризуйте складові плану захисту інформації та організаційні і первинні технічні заходи захисту інформації?
24. Дайте характеристику організаційної складової обстеження об`єктів інформаційної діяльності Підприємства. Здійснення первинних технічних заходів захисту інформації
25. Визначення терміну «інформація з обмеженим доступом». У яких випадках інформацф з обмеженим доступом може бути поширена без згоди її Власника?
26. Охарактеризуйте види інформації з обмеженим доступом. Розкрийте зміст термінів «конфіденційна інформація» і «таємна інформація».
27. Охарактеризуйте види конфіденційної і таємної інформаціїї.
28. Повноваження Верховної Ради України і функції РНБО України у мирний час в сфері охорони державної таємниці?
29. Дайте характеристику функцій Кабінету Міністрів України та функцій органів судової влади у сфері охорони державної таємниці. Основні завдання Департамента спеціальних телекомунікаціних систем
30. Що відноситься до повноважень із контролю за охороною державної таємниці, яке здійснює СБ України? Дозвільні повноваження СБ України в сфері охорони державної таємниці.
31. Основи віднесення (або не віднесення) інформації до державної таємниці в Україні. Державна експертиза з питань таємниць в Україні.
32. Права, обов`язки і відповідальність Державного експерта з питань таємниць в Україні. Основи засекречування та розсекречування інформації в Україні.
33. Організаційно-правові заходи з охорони державної таємниці в Україні.
34. Основні розділи «Типового положення про підрозділ захисту інформації». Мета створення та основні завдання підрозділу захисту інформації на Підприємстві.

35. Організація навчання персоналу із забезпеченню захисту інформації. Права і основні функці СЗІ. Основні обов`язки керівника та співробітників СЗІ.
36. Підрозділи і зовнішні організації, з якими взаємодіє СЗІ. Штатний розклад і структуру СЗІ і організація заходів СЗІ на Підприємстві.
37. Що є предметом злочинів в сфері інформаційно-комунікаційних технологій та які існують категорії осіб, що вчиняють комп`ютерні злочини? Охарактеризуйте загальну класифікацію комп`ютерних злочинів в Україні.
38. В чому полягає суть наступних комп`ютерних злочинів: несанкціонований доступ та перехоплення ((QA); Охарактеризуйте порушення типу «зміна комп`ютерних даних».
39. Що є предметом злочинів в сфері інформаційно-комунікаційних технологій та які існують категорії осіб, що вчиняють комп`ютерні злочини? Комерційна таємниця в Україні та комп`ютерні злочини, пов`язані з нею.
40. В чому полягають основні порушення в організаційній роботі із засобами захисту інформаціх згідно постанови НБУ №280 «Про затвердження правил організації захисту електронних банківських документів» від 10.06.1999 р.
41. Охарактеризуйте профілактичні заходи та організаційну роботу з попередження та розкриття комп`ютерних злочинів на державному рівні України.
42. Що необхідно робити при виявленні несанкціонованого доступу до комп`ютеррів та їх мереж в Установі чи на Підприємстві? Охарактеризуйте основнвні обставини, що підлягають встановленню при розслідуванні комп`ютерних злочинів.
43. Організаційна робота з виявлення несанкціонованого втручання в роботу інформаційно-комунікаційної системи та несанкціонованого знищення інформації, яка в ній міститься.
44. Організаційна робота з виявлення несанкціонованого вилучення комп`ютерної інформації, яка зберігалась в пристроях довгострокового зберігання . Організаційна робота при встановленні порушень правил експлуатації комп`ютерів, їх мереж автоматизованих систем або мереж електрозв`язку.
45. Організаційна робота з виявлення несанкціонованого втручання в роботу комп`ютерів, їх мереж автоматизованих систем або мереж електрозв`язку та при підтвердженні факту несанкціонованих дій з інформацією, що обробляється.

6. Теми рефератів

1. Побудова ефективних рубежів територіального захисту і доступ до незахищених інформаційних ресурсів.
2. Протидія розкраданню документів та електронних носів інформації.
3. Методи протидії візуальному перехопленню інформація, яка введена на екрани моніторів.
4. Боротьба з прослуховуванням (методика, будова і оптимізація захисних бар`єрів).
5. Боротьба з перехопленням електромагнітних випромінювань інформаційно-комунікац3ійних систем.
6. Будова і принцип дії систем охоронного телебаченняна.
7. Методи оптимізації і контролю за роботою систем охоронного телебачення.
8. Заземлення: методи розрахунку, будова і використання.
9. Охоронне освітлення: методи розрахунку, будова і використання.
10. Методи розрахунку та оптимізації систем екранування приміщень з комп`.терними системами від витоку електро-магнітних випромінювань.
11. Спеціальні інженерно-технвічні споруди, інформаційних систем , які передають кофіденціцйну інформацію.
12. Системи оптичного і акустичного екранування носіїв інформації з обмеженим доступом.
13. Атестація систем захистту інформації на Підприємстві.
14. Порядок і методи контролю за станом фізичного захисту інформаційно-комунікаційних систем.
15. Основи технічного захисту інформації в системах телефонного і телеграфного зв`язку.
16. Захист інформації в системах звукопідсилення, звукозапису та звуковідтворення.
17. Основи будови та розрахунку сучасних систем протипожежної сигналізації.
18. Захист інформації в системах перетворення, опрацювання, пересилання і приймання відеоканалів, що містять конфіденційну інформацію.
19. Біометричні системи доступу до захищених інформаційних систем.
20. Державна експеритиза і сертифікація засобів технічного захисту в Росії.
21. Мінімальні стандарти організаційних основ захисту інформації з гобмеженим доступом в країнах НАТО і ЄС.

22. Стандарт ISO/IES (27001: «Інформаційні технології – Методика безпеки – Система менеджменту – Вимоги» (стандарт, за яким організація може бути сертифікована).
23. Стандарт ISO/IES (27005:2008 «Інформаційні технології – Методика безпеки – Управління ризиками інформаційної безпеки» (стандарт, що надає рекомендації з управління безпекою на основі підходу управління ризиками).
24. Стандарт ISO/IES (27006:2007 «Інформаційні технології – Методика безпеки – Вимоги до організацій, що проводять аудит і організацію систем менеджменту інформаційної безпеки» (настанови з акредитації сертифікаційних організацій).
25. Вимоги до обладнання, приладів і метрологічного забезпечення робіт в комплексній інформаційно-комунікаційній системі захисту інформації.
26. Американська та японська моделі управління персоналом Підприємства.
27. Загальні критерії, що висуваються до співробітників служби безпеки типової фірми США.
28. Критерії та основні підбору працівників для виробництва у США.
29. Тренінг з питань захисту комерційної таємниці та забезпечення безпеки фірми в США.
30. Проблемно-орієнтовані семінари в галузі захисту комерційної таємниці фірм (на прикладі США).

7. **Тести**

Контрольна робота №1

1.Зміст і послідовність робіт з протидії загрозам інформації полягає в наступному:

А - обстеженні Підприємства;

Б – прийманні робіт з ТЗІ;

В – атестації засобів забезпечення інформаційної діяльності на відповідність вимогам до нормативних документів з ТЗІ;

2.Технічному захисту підлягає наступна інформація:

А – відкрита інформація, носіями якої є сигнали, що утворюються в результаті роботи технічних засобів відображення інформації;

Б – інформація з обмеженим доступом, носіями якої є поля й сигнали, що утворюються в результаті технічних засобів пересилання, опрацювання, зберігання. Відображення інформації здійснюється за допомогою основних технічних засобів (ОТЗ), а також за допомогою допоміжних технічних засобів (ДТЗ).

В – таємна інформація в комп`ютерних мережах.

3.*До технічних засобів пересилання, опрацювання, зберігання і відображення інформації належить:*

А – засоби і системи звукопідсилення, звукозапису і звуковідтворення;

Б – апаратура перетворення відеоканалів, яка містить факсимільну інформацію;

В – засоби і системи технологічного зв`язку.

4.Допоміжні технічні засоби і системи це:

А – засоби і системи спеціальної охоронної сигналізації;

Б – засоби і системи звуковідтворення;

В – засоби і системи годинофікації..

5.***Елементи ОТЗ і ДТЗ, як зосереджені (апаратура і її блоки) чи випадкові антени (кабельні лінії та проводи) це:***

А – елементи заземлення і електроживлення;

Б – комутаційні пристрої;

В – кабельні мережі та розводки, які сполучають обладнання.

6.Організаційні заходи щодо технічного захисту інформації це:

А – визначення переліку відомостей з обмеженим доступом, які підлягають технічному захисту;
Б – визначення технічних засобів, застосування яких не обгрунтоване службовою і виробничою необхістю і які підлягають демонтажу;
В – визначення систем, які потребують переобладнання кабельних мереж.

7. У акті обстеження АС вказується:
А – пернелік ОТЗ, розміщених у виділених приміщеннях;
Б – схеми прокладених кабелів, проводів та електричних кіл;
В – перелік технічних засобів, які підлягають демонтажу.

8.Блокування ліній зв`язку здійснюється наступними способами:
А – демонтажем технічних засобів, кабелів, кіл, проводів, що виходять за межі виділених приміщень;
Б – встановлення найпростіших схем захисту;
В – видалення за межі виділених приміщень окремих елементів технічних засобів, які можуть бути джерелом виникнення каналу витоку інформації.

9.Запобігання витоку інформації з обмеженим доступом ІзОД через діючі системи гучномовного зв`язку здійснюється наступним чином:
А – встановленням у викличних колах вимикачів для розриву електричних кіл;
Б – запобіганням можливості відключення живлення мікрофонних підсилювачів;
В – встановлення найпростіших пристроїв захисту.

10.Заходи блокування витоку інформації з обмеженим доступом через системи електронної оргтехніки це:
А – розташування зазначеної системи у середині контрольованої території без винесення окремих компонентів за її межі;
Б - розташування зазначеної системи у середині контрольованої території з винесенням окремих компонентів за її межі
В – електроживлення систем від трансформаторної підстанції, яка знаходиться всередині контрольованої території.

11. До засобів технічного захисту інформації належать:

А–фільтри мережеві для блокування витоку мовної інформації з обмеженими каналами електроживлення;

Б – генератори зашумлення;

В – екрановані камери спеціальної розробки.

12.Захист ІзОД від витоку кабелями і проводами рекомдується здійснювати наступним чином:

А – застосовувати заземлені конструкції;

Б – застосовувати екранування ІКС;

В – використовувати спільне прокладання кабелів ОТЗ та ДТЗ.

13. Перехрещення кабельних трас різного призначення рекомендовано проводити під кутом:

А – $\alpha = 45^0$;

Б - $\alpha = 90^0$;

В - $\alpha = 135^0$.

14.Заземлення ОТЗ слід здійснювати так:

А – від загального контуру заземлення в межах контрольованої території;

Б - від загального контуру заземлення за межами контрольованої території;

В - від часткового контуру заземлення в межах контрольованої території;

15.Екрани кабелів:

А – не повинні мати електричного контакту з іншими металоконструкціями;

Б - повинні мати електричний контакт з металоконструкціями;

В – можуть використовуватись як другий провід сигнального каналу чи каналу живлення.

Контрольна робота №2

1.Метою зовнішнього аудиту безпеки інформації є:

А – оцінка максимального рівня захищеності інформаційної системи;

Б – локалізація вузьких місць у системі захисту інформаційної системи;

В – побудова моделі ризиків і порушника для АС.

2. Метою внутрішнього аудиту безпеки інформації є:

А – постановка задач для персоналу щодо збереження захисту інформації;
Б – оцінка відповідності інформаційної системи існуючим стандартам в області інформаційної безпеки;
В – участь у розборі інцидентів, пов`язаних із порушенням інформаційної безпеки.

3.Етапи аудиту безпеки інформаційних систем:
А – ініціювання процедури аудиту;
Б – вироблення рекомендацій;
В – підготовка комплексної угоди про безпеку інформації.

4.Організаційні питання на етапі ініціювання процедури аудиту:
А – аудитором повинен бути підготовлений і погоджений із керівництвом план проведення аудиту;
Б – права аудитора повинні бути максимальними;
В – обов`язки аудитора повинні бути фіксовані в його посадовій інструкції.

5.В межах проведення обстеження при аудиті повинно бути:
А – список фізичних, програмових та інформаційних ресурсів, які підлягають процедурі обстеження;
Б – результати аналізу ризиків;
В – критичні площі.

6.Інформація, що необхідна аудитору:
А – структурна схема інформаційної системи;
Б – схема інформаційних потоків;
В – схема розташування складових ІКС.

7.Типові питання, які задає аудитор опитуваним:
А – хто власник інформації?;
Б – хто провайдер послуг?
В – які послуги і яким чином надаються користувачам?

8.Аналіз даних аудиту направлений на:
А – визначення структури КСЗІ;
Б – складання ранжованого списку загроз безпеці інформації;
В – оцінку фінансових потоків у АС.

9.Категорії інформації із виділенням груп доступу при виробленні рекомендацій аудитором:

А – заборонено зміни;

Б – заборонено вилучення;

В – заборонено читання.

10.Аудиторський звіт повинен містити:

А – вказівку меж проведення аудиту і методів аудиту;

Б – рекомендації аудитора з усунення виявлених недоліків і вдосконалення системи захисту інформації;

В – характеристику КСЗІ інформаційної системи.

11.В аудиторському звіті для кожного комп`ютера або сервера повинні відображатись наступні відомості:

А – у якому домені або робочій групі знаходиться комп`ютер;

Б – список файлів з інформацією із грифом «таємно», «для службового користування»;

В – відповідальна за комп`ютер особа.

12. В аудиторському звіті для кожної мережі і підмережі повинні відображатись наступні відомості:

А – список усії мережевих пристроїв;

Б – ємність і вартість мережі;

В – список усіх апаратних пристроїв, які забезпечують конфіденційність роботи.

13. В аудиторському звіті для кожного співробітника повинні відображатись наступні дані:

А – список комп`ятерів, до яких має доступ співробітник;

Б – знання співробітником вимог безпеки інформації ;

В – список комп`ятерів, до яких не має доступу співробітник.

14.Типовий етичний кодекс аудитора інформаційних систем передбачає, що аудитор буде:

А – дотримуватися конфіденційності інформації, одержаної при виконання своїх посадових обов`язків;

Б – не інформувати всі зацікавлені сторони про результати аудиту;

В – вдосконалювати свої особисті професійні якості.

15.Зміст і послідовність робіт з протидії загрозам полягає в :

А – проведенні обстеження Підприємства;

Б – розробленні первинних технічних заходів без використання засобів забезпечення ТЗІ;
В – прийнанні робіт з ТЗІ.

Контрольна робота №3

1.Рівень захисту від некоректного використання ресурсів системи має наступні механізми:

А – підтримка цілісності та несуперечливості даних;
Б – копіювання ділянок оперативної пам`яті;
В – попередження користувача перед проведенням небезпечних операцій.

2.На рівні внесення інформаційної та функціональної надмірності здійснюється:

А – тестування і самотестування;
Б – резервування інформації;
В – ізолювання ділянок оперативної пам`яті.

3.Схема здійснення доступу включає наступне:

А – суб`єкт, метод доступу, об`єкт;
Б - суб`єкт, об`єкт, програмне забезпечення;
В - суб`єкт доступу, метод доступу до об`акта.

4.Методи доступу, які залежать від типу об`акта це:

А – записування;
Б – множення;
В – додавання.

5.Суть мандатного керування доступом полягає:

А – у тому, що з кожним об`єктом, пасивним і активним (суб`єктом) асоціюють «мітку безпеки», яка визначає рівень цього об`єкта у деякій ієрархії рівнів;
Б – у тому, що з кожним об`єктом асоціюють спеціальну програму захисту інформації;
В – у тому, що кожному користувачеві присвоюється спеціальний код.

6.До способів підтвердження істинності користувача належать механізми перевірки:

А – інформації, що відома лише користувачу та системі автентифікації (паролі, ідентифікаційні коди тощо);
Б – додаткові відомості, для таємного зберігання яких застосовуються знімні пристрої (смарт-картки, ключі тощо);

В – інформації про КСЗІ.

7. Криптографічна підсистема забезпечує наступні механізми захисту:

А – шифрування і дешифрування даних;
Б – накладання електронного цифрового підпису;
В- накладання електронного цифрового підпису.

8.Можливості системи електронного конфіденційного документообігу це:

А –створення електронних документів з використанням текстових редакторів;
Б – створення електронних документів за допомогою криптографічного програмового забезпечення;
В – створення електронних документів за допомогою інших електронних даних.

9.До реквізитів реєстраційної картки електронного документа належить:

А – міра конфіденційності;
Б – дата створення, одержання і виконання;
В – кількість аркушів.

10.Пошук електронних документів здійснюють за:

А – ключовими словами;
Б – тематикою і проблематикою;
В – реквізитами.

11.Можливості системи конденфіденційного електронного інформаційного сховища:

А – організація маловитратної технології видачі документів співробітникам та повернення документів у сховище;
Б – збільшення кількості документів, що одночасно знаходяться у виконавця за рахунок оперативного одержання їх із сховища;
В – відслідковування руху документів виданих співробітникам, контроль і забезпечення їх повернення і архівування виданих електронних клопій.

12.Системи сполучення електронного і паперового діловодства складаються із:

А – систем перекладу паперового документа в електронний і навпаки;

Б – системи електронного контролю за електронним документообігом;
В – системи послідовного обігу документів.

13.Блоки систем захисту конфіденційного електронного діловодства:

А- блок організаційних методів захисту електронного діловодства;
Б – блок методів захисту електронного діловодства, пов`язаний з людським чинником і вирішенням кадрових проблем;
В – блок технічних засобів захисту приміщень з АС.

14.Рубежі технічних (програмових) засобів захисту електронного діловодства:

А – системи захисту інформації програмовим забезпеченням Інтернету;
Б – системи захисту інформації, вбудовані в систему електронного діловодства;
В – системи захисту інформації, пов`язані з нейтралізацією побічних електромагнітних випромінювань і наведень.

15. Блок технічних засобів захисту електронного діловодства повинен передбачати:

А – захист комп`ютерної інформації від несанкціонованого доступу;
Б – криптографічний захист комп`ютерної інформації на магнітних носіях, в тому числі створення захищених «цифрових сейфів» користувачів сервера.
В - створення захищених «цифрових сейфів» користувачів сервера.

Контрольна робота №4

1.Типи категорій об`єктів інформаційної діяльності:

А – перша категорія - об`єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю з грифом «цілком таємно»;
Б – друга категорія - об`єкти, в яких циркулює інформація, що містить відомості з грифом «особливої важливості»;
В-до четвертої категорії належать об`єкти, в яких циркулює конфіденційна інформація.

2.Що визначає комісія з категоріювання об`єктів інформаційної діяльності ?

А – діапазон грифів секретності інформації, яка циркулює на об`єкті;

Б – підставу для категоріювання (первинне, планове тощо);

В – нижній гриф секретності інформації, яка циркулює на об`єкті.

3.Реквізити кожного матеріального носія секретної інформації повинні містити:

А – гриф секретності («особливо важливо». «цілком таємно» тощо);

Б – дату і строк засекречування матеріального носія секретної інформації;

В – фамілію, ім.`я та по-батькові працівника, що надав зазначений гриф.

4.Звід відомостей, що становить державну таємницю формує:

А – МВС України та публікує в пресі;

Б – і публікує в офіційних виданнях Служба безпеки України на підставі рішень державних експертів з питань таємниць.

В – та публікує Кабінет Міністрів України за поданням Служби безпеки України.

5.Модель порушника – це:

А – всебічна структурна характеристика, яку разом з моделлю загроз використовують під час розроблення політики безпеки інформації;

Б – характеристика порушника, який здійснив несанкціонований доступ;

В – опис методів несанкціонованого проникнення в АС.

6.Категорії порушників:

А – користувачі;

Б – зовнішні порушники;

В – співробітники служби безпеки.

7.Мета порушника безпеки інформації:

А –отримання інформації з грифом «таємно»;

Б – отримання можливості вносити зміни в інформаційні потоки відповідно до своїх намірів;

В – завдання збитків шляхом знищення інформаційних цінностей.

8. Повноваження порушника в АС це:
А – запуск фіксованого набору задач (програм);
Б – внесення змін у конфігурацію системи;
В –зміна конфігурації апаратних засобів;

9.До рівнів інформаційно-комунікаційної системи належать:
А – КСЗІ;
Б – бази даних;
В – мережні послуги.

10.Рекомендованою є наступна структура опису порушника:
А – категорія осіб, до яких може належати порушник;
Б – повноваження порушника;
В - програмове забезпечення порушника.

11.До функціонального сервісу безпеки інформації належать:
А – доступність;
Б – причетність до відправлення інформації;
В – конфіденційність.

12.Механізми, які реалізуються на рівні захисту від несанкціонованого доступу:
А – автентифікація;
Б – квоти;
В – захист програм від копіювання.

13.Рівні захисту від несанкціонованого використання ресурсів реалізуєть:
А –захист від комп`ютерних вірусів;
Б – шифрування;
В – контроль за виділенням ресурсів та квот.

14.Зміст і послідовність робіт з протидії загрозам інформації полягає в наступному:
А - обстеженні Підприємства;
Б – прийманні робіт з ТЗІ;
В – атестації засобів забезпечення інформаційної діяльності на відповідність вимогам до нормативних документів з ТЗІ;

15.Технічному захисту підлягає наступна інформація:

А – відкрита інформація, носіями якої є сигнали, що утворюються в результаті роботи технічних засобів відображення інформації;

Б – інформація з обмеженим доступом, носіями якої є поля й сигнали, що утворюються в результаті технічних засобів пересилання, опрацювання, зберігання. Відображення інформації здійснюється за допомогою основних технічних засобів (ОТЗ), а також за допомогою допоміжних технічних засобів (ДТЗ).

В – таємна інформація в комп`ютерних мережах.

Контрольна робота №5

1.Зміст і послідовність робіт з протидії загрозам інформації полягає в наступному:

А - обстеженні Підприємства;

Б – прийманні робіт з ТЗІ;

В – атестації засобів забезпечення інформаційної діяльності на відповідність вимогам до нормативних документів з ТЗІ;

2.Технічному захисту підлягає наступна інформація:

А – відкрита інформація, носіями якої є сигнали, що утворюються в результаті роботи технічних засобів відображення інформації;

Б – інформація з обмеженим доступом, носіями якої є поля й сигнали, що утворюються в результаті технічних засобів пересилання, опрацювання, зберігання. Відображення інформації здійснюється за допомогою основних технічних засобів (ОТЗ), а також за допомогою допоміжних технічних засобів (ДТЗ).

В – таємна інформація в комп`ютерних мережах.

3.Оброблення інформації це:

А – процес перетворення, зберігання і знищення інформації, який здійснюється за допомогою програмових засобів;

Б – вся сукупність операцій, що здійснюються за допомогою технічних і програмових засобів, включаючи обмін інформацією каналами передачі даних;

В – сукупність операцій, що здійснюються за допомогою технічних засобів.

4.Захист інформації це:

А – сукупність організаційно-технічних заходів і правових норм для запобігання шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

Б – сукупність правових норм із запобігання витоку інформації;

В – набір організаційних заходів із запобігання шкоди інтересам власників інформації або АС.

5.Несанкціонований доступ до інформації являє собою:

А – доступ, який здійснюється з порушенням антивірусного забезпечення;

Б – доступ до інформації, який здійснюється з порушенням встановлених в АС правил розмежування доступу;

В – доступ до конфіденційної інформації з порушенням правил.

6.Порушник це:

А – юридична особа, що навмисно здійснює неправомірні дії щодо АС та інформації, що в ній міститься;

Б – фізична особа, яка ненавмисно здійснює неправомірні дії щодо АС;

В – фізична або юридична особа, що навмисно здійснює неправомірні дії щодо АС та інформації, що в ній міститься.

7.Витік інформації це:

А – процес, в результаті якого інформація стає доступною довільному користувачу АС;

Б – результати дій порушника, внаслідок яких інформація стає відомою суб`єктам, що не мають права доступу до неї;

В – процес, який блокує антивірусне забезпечення КСЗІ.

8.Порушення роботи АС це:

А – перекручування даних, що обробляються в АС;

Б – дії чи обставини, яки призводять до спотворення процесу оброблення інформації;

В – дії, які викликають спотворення даних в АС.

9.Суб`єкти відносин, що пов`язані з обробленням інформації в АС це:

А –власники АС або уповноважені ними особи;

Б – власники інформації;

В – користувачі АС.

10.Можливі загрози роботі інформаційних систем це:
А – стихійні лиха і аварії;
Б – наслідки помилок проектування компонентів АС;
В – стихійні лиха і політична нестабільність в країні.

11.До ненавмисних загроз інформації відноситься:
А – випадкове зараження вірусом;
Б – розкарадання носіїв інформації;
В – ненавмисне відключення устаткування чи зміна режимів роботи пристроїв і програм.

12.Навмисні загрози інформації це:
А – дії з дезорганізації функціонування системи оброблення інформації;
Б – незаконне заволодіння паролями;
В – ігнорування організаційних обмежень.

13. Класифікація атак за Пітером Меллом це:
А – локальна відмова в обслуговуванні;
Б – активне прослуховування мережі;
В – віддалене проникнення.

14.Для чого використовують методику класифікації загроз STRIDE?
А – для побудови моделі порушника;
Б – для побудови моделі загроз під час розроблення програмного забезпечення;
В - для побудови матриці ризику загрозам інформації в АС.

15.До методики класифікації загроз інформації STRIDE відноситься:
А – відмова від авторства;
Б – модифікація даних;
В – сканування мережі.

Контрольна робота №6

1.Вади захисту це:
А – сукупність причин, умов та обставин, наявність яких може привести до порушення нормального функціонування системи або політики безпеки інформації;

Б – особливості побудови програмових засобів захисту, що за певних обставин спричинюють їхню нездатність протистояти загрозам і виконувати свої функції;
В – окремий випадок уразливості системи.

2.Порушник це:
А – фізична особа, що порушує політику безпеки;
Б - фізична особа, що ненавмисно здійснює порушення антивірусного забезпечення АС;
В – особа, яка навмисно порушує правила антивірусного забезпечення АС.

3. Модель порушника це:
А – опис методики порушення безпеки інформації;
Б – абстрактний формалізований чи неформалізований опис порушника;
В - абстрактний формалізований чи неформалізований опис методів і засобів здійснення загроз.

4.Захищена комп`стерна система це:
А - комп`ютерна система, яка здатна забезпечувати захист інформації від визначених загроз;
Б - комп`стерна система, яка знаходиться під захистом антивірусних програм;
В - комп`стерна система, що протидіє витоку інформації технічними каналами.

5.Комплексна система захисту інформації (КСЗІ) це:
А - сукупність організаційних, інженерних і програмово-апаратних засобів, що забезпечують захист інформації в ІКС;
Б – сукупність програмових засобів, що можуть забезпечувати антивірусний захист;
В – сукупність технічних заходів захисту інформації.

6.Об`єкт системи – це елемент ресурсів обчислювальної системи, який знаходиться під керуванням КЗЗ, характеризується визначеними атрибутами й повноваженнями і має наступні види:
А – пасивні об`єкти, об`єкти-користувачі, активні об`єкти;
Б - пасивні об`єкти, об`єкти-користувачі, об`єкти-процеси;
В - об`єкти-процеси, активні об`єкти;

7.Доступ це:

А – взаємодія двох об`єктів обчислювальної системи, коли один із них виконує роботу над іншим;

Б – взаємодія множини об`єктів, коли перший об`єкт виконує дії над іншими;

В – можливість досягнення доступу до конфіденційної інформації.

8.Правила розмежування доступу це:

А – порядок доступу користувачів до інформаційних об`єктів;

Б – складова політики безпеки, яка регламентує правила доступу користувачів і процесів до пасивних об`єктів.

В – складова політики моделі загроз.

9.Несанкціонований доступ це:

А – доступ, що відбувається з порушенням антивірусного забезпечення;

Б – доступ, який здійснюється з порушенням політики безпеки, тобто з порушенням правил розмежування доступу (ПРД);

В – доступ, що протирічить моделі загроз.

10.Ідентифікація це:

А – процес впорядкування інформаційних об`єктів за їх іменами;

Б – процес встановлення інформаційних об`єктів за інформаційною ємністю;

В – процес розпізнавання об`єктів інформаційної системи за їх мітками безпеки.

11.Автентифікація це:

А – перевірка запропонованого ідентифікатора на відповідність об`єкту, пересвідчення в його справжності;

Б – перевірка інформаційної ємності ІКС;

В – перевірка відповідності КСЗІ стандартам безпеки інформації.

12.Авторизація це:

А – процедура встановлення справжності користувача;

Б – процедура надання користувачу визначених повноважень у системі;

В - перевірка інформаційної ємності ІКС.

13.Кваліфікаційний аналіз це:

А – аналіз ІКС з метою визначення рівня її захищеності та відповідності вимогам безпеки на основі критеріїв стандарту безпеки;

Б – аналіз КСЗІ на її надійність;

В – аналіз КЗЗ з метою встановлення її відповідності моделі безпеки інформації.

14.Автоматизована система це:

А – система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки, а також методи і процедури та відповідне програмне забезпечення;

Б – системи, що здійснюють обробку інформації;

В – системи, які дозволяють застосувати програмне забезпечення при обробці інформації.

15. Інформація в АС це:

А – сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх логічного представлення;

Б – сукупність програм, які використовуються в АС;

В – набір даних, що використовується в КСЗІ.

Контрольна робота №7

1.Сфера управління, як специфічний вид соціальної діяльності це:

А – планування, тобто визначення цілей і задач підприємства, а також шляхів їх реалізації;

Б – контроль за виробничою діяльністю;

В – управління персоналом.

2.Істотною ознакою, що визначає працездатність співробітників є відносини в діапазоні:

А – конфронтація – підлеглість;

Б – співробітництво – конфронтація;

В – співробітництво – керівництво.

3.Робочими поняттями в поясненні організаційної поведінки є:

А – мотиви, стимули, мотивація;

Б –підлеглість;

В – впорядкованість.

4.До основних задач організаційної поведінки належить:

А – виявлення поведінкових відносин в колективі;

Б – створення атмосфери творчого потенціалу працівників;

В – забезпечення сприятливого температурного режиму в приміщеннях.

5.Автоматизована система з оброблення інформації поєднує в собі:

А – інформацію, що обробляється і персонал;

Б – обчислювальну систему і фізичне середовище;

В – обчислювальну систему, фізичне середовище, персонал та інформацію, що обробляється.

6.Мета захисту інформації це:

А – забезпечення цілісності інформації;

Б – збереження цінності інформації для її власника;

В – забезпечення доступу і не спотворення важливої інформації.

7.Політика безпеки інформації це:

А – сукупність рекомендацій із оброблення і збереження інформації;

Б – набір стандартів в галузі захисту інформації;

В - сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації і ІКС.

8.Безпека інформації це:

А – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації;

Б – стан інформації, коли імовірність несанкціонованого доступу до неї наближається до нуля;

В – стан інформації, коли відсутня можливість блокування доступу.

9. Конфіденційність це:

А – властивість інформації, завдяки якій лише вповноважені користувачі мають змогу її отримати;

Б – властивість інформації зберігатись неспотвореною невизначено довгий час;

В – властивість інформації бути доступною користувачам.

10.Головні властивості інформації, збереження яких гарантує збереження цінності інформаційних ресурсів це:

А – закритість і цілісність;
Б – конфіденційність, цілісність і доступність;
В - цілісність і доступність.

11.Цілісність інформації це:

А – властивість інформації, завдяки якій лише вповноважені користувачі мають змогу її отримати;
Б – властивість інформації бути неспотвореною при передачі на великі віддалі;
В - властивість інформації бути доступною для кодування.

12. Доступність інформації це:

А – властивість інформації, завдяки якій лише уповноважені користувачі можуть її використовувати згідно правил, що встановлені на Підприємстві;
Б - властивість інформації, завдяки якій лише уповноважені користувачі можуть її використовувати згідно правил, що встановлені політикою безпеки, не очікуючи довше заданого (невеликого) проміжку часу;
В - властивість інформації, завдяки якій любі користувачі швидко одержують інформацію, що їх цікавить.

13.Несприятливий вплив це:

А – вплив, що приводить до зменшення цінності інформаційних ресурсів;
Б - вплив, що приводить до блокування роботи ІКС;
В – вплив, який блокує антивірусне програмне забезпечення.

14.Загроза інформації це:

А – будь-які обставини і події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку ІКС;
Б – довільний потенційно можливий несприятливий вплив;
В – порушення антивірусного захисту ІКС;

15. Атака це:

А – порушення безпеки інформації в ІКС;
Б – спроба реалізації загрози;
В – проникнення в ІКС без дозволу.

Контрольна робота №8

1.Під захисним заземленням розуміють:

А – з`єднання металічних струмоведучих частин електроустановки з землею через заземлюючі провідники;

Б - з`єднання неструмоведучих частин електроустановки з землею кабелем з подвійним екраном;

В - з`єднання металічних неструмоведучих частин електроустановки з землею через заземлюючі провідники і заземлювач для створення між цими частинами і землею малого опору.

2.Принцип роботи захисного заземлення базується на:

А – збільшенні напруги дотику і спрацюванні автоматичного відмикання напруги;

Б – на зменшенні до безпечних значень напруги дотику і крокової напруги, що досягається шляхом зменшення опору заземлення;

В – на зменшенні крокової напруги, що досягається шляхом зменшення діаметра провідників заземлення.

3.Захисне заземлення застосовують:

А – у трифазних мережах із заземленою нейтраллю та напругою до 1000 В, а вище 1000 В – при довільному режимі роботи нейтралі;

Б – у трифазних мережах із напругою вищою за 1000 В;

В – в електроустановках з напругою меншою за 42 В.

4.Величина струму, що відгалужується з системи «заземлений корпус-заземлюючий пристрій» і яка проходить через тіло людини залежить:

А – від величини струму замикання на землю;

Б – опору розтікання струму в землі заземлюючого пристрою;

В – повного опору в колі «людина – земля».

5.Повний опір у колі «людина-земля» складається з:

А - опору людини, опору взуття і опору розтікання струму від підошви взуття в землю;

Б – опору заземлювачів і опору людини за напрямком «рука-рука»;

В – опору взуття і опору розтікання струму.

6.Питомий опір грунту залежить від:

А – його будови, вмісту в ньому розчинених речовин, вологи, а також від температури повітря;

Б – його питомої ваги і густини;
В – вмісту вологи в грунті.

7. Питомий електричний опір (Ом м) різних типів грунтів:
А – чорнозем 9 – 53;
Б – глина 15-100;
В – суглинок 150-400.

8.Розрахунок захисного заземлення методом коефіцієнтів використання здійснюють:
А – при неоднорідній структурі грунту;
Б – при однорідній структурі грунту для простих заземлювачів;
В - при однорідній структурі грунту для складних заземлювачів.

9. Метою розрахунку системи заземлення методом коефіцієнтів використання є:
А – визначення кількості електродів заземлення і заземлюючих провідників, їх розмірів і схеми розміщення в грунті;
Б – визначення опору заземлення;
В – оптимізація схеми і кількості електродів заземлення в грунті.

10. Допустиме значення опору захисного заземлення в електротехнічних установках:
А – в установках з великим струмом замикання на землю – 0,75 Ом;
Б – всіх інших установках – 4.0 Ом;
В –в установках з великим струмом замикання на землю ($I_з$ > 500 А) – 0,5 Ом.

11. Види кваліфікаційного аналізу:
А – акредитація (КЗЗ, КСЗІ);
Б – сертифікація;
В – дослідна експлуатація.

12.У державній експертизі приймають участь:
А – організатори експертизи;
Б – експерти-фізичні особи, які виконують експертні роботи;
В – власники КСЗІ.

13.Державну експертизу повинні проходити наступні об`єкти:
А – КСЗІ, як невід`ємна частина об`єктів інформаційної діяльності;

Б – адміністративні будівлі власника АС;
В – матриця ризику для КЗЗ.

14.Види державної експертизи ІКС:
А – контрольна;
Б – додаткова;
В – основна.

15. План проведення державної експертизи містить наступні пункти:
А – організатор призначає експертів, яких буде залучено до виконання робіт;
Б – протокол експертизи підпису керівник Адміністрації Держспецзв`язку;
В – організатор складає і підписує експертний висновок, який визначає відповідність об`єкта експертизи експертним вимогам НД ЕЗІ.

Контрольна робота №9.

1.Екранування електромагнітного випромінювання в 10-30 разів забезпечується використанням:
А – одинарної мідної сітки з комірками 2,5 мм;
Б – подвійної сітки із свинцю з комірками 5 мм;
В –екрану з оцинкованої сталі товщиною 0,51 мм і більше.

2.Для чого в системах електромагнітного екранування використовують пружинну гребінку з фосфористої бронзи ?
А – для екранування підлоги;
Б – для екранування стелі;
В – для екранування дверей і вікон приміщень, де здійснюється захист інформації від витоку технічними каналами.

3.Яким чином екранують вікна ?
А – одним чи двома листами цинкованої сталі товщиною 0,51 мм і більше;
Б – одним чи двома прошарками мідної сітки з комірками не більшими за 2х2 мм і відстанню між прошарками не меншою 50 мм;
В - одним чи двома прошарками мідної сітки з комірками не більшими за 2х2 мм і відстанню між прошарками не меншою 1 см.

4.Мережеві фільтри в ланцюгах живлення технічних засобів передавання інформації виконують функції:

А – захист апаратури від зовнішніх перешкод;

Б - захист апаратури від внутрішніх перешкод;

В – захист від наведень самої апаратури.

5.При виборі фільтрів враховується:

А – міра екранування фільтра від сторонніх полів;

Б – механічні характеристики фільтра;

В – допустимі значення реактивної складової струму на другій гармоніці частоти напруги живлення.

6.Причини витоку електромагнітного випромінювання з ІКС:

А – неповністю екранований корпус;

Б – проникнення електричних полів через отвори в плетеній оболонці кабелів;

В – проникнення електричних полів через скляні вікна.

7.Вплив опору зв`язку коаксіального кабеля на його екрануючі властивості:

А – чим менший опір зв`язку кабеля, тим краща його екрануюча дія;

Б - чим більший опір зв`язку кабеля, тим краща його екрануюча дія;

В – опір зв`язку повинен точно співпадати з вихідним опором ІКС.

8. Екранування змінного магнітного поля засновано:

А – на протіканні струму в петлі, яка утворена заземленою на кінцях, трубою і землею;

Б – протіканні струму по заземленні та компенсації струмів в контурі заземлення.

В - протіканні струму по заземленні.

9.Зміщення потенціалу в імпульсному генераторі поряд з наведеними та індукованими електрорушійними силами є:

А – причинами високого опору заземлення для ВЧ сигналів;

Б – причинами появи значних завад;

В – причинами покращення екрануючої дії оболонок кабелів.

10. При оптимальному варіанті заземлення:

А – струми в оболонках кабелів і по корпусам приладів повинні бути в межах 1 - 0,5 А;

Б - струми в оболонках кабелів і по корпусам приладів повинні бути порівняно малими;
В - струми в оболонках кабелів і по корпусам приладів повинні перевищувати 1 А.

11.Рекомендована схема імпульсної чи ВЧ частини АС повинна включати:
А – кабельні канали, що не перетинаються, а лише розгалужуються;
Б – кабельні канали, які розгалужуються і перетинаються під кутом 90^0;
В - кабельні канали, що не розгалужуються, а лише перетинаються;

12.Найчастіше в системах заземлення використовуються:
А – вертикально занурені в землю сталеві труби довжиною 2 - 3 метри і діаметром 35-50 мм;
Б – горизонтально занурені на глибині 50 см труби довжиною 5 м і діаметром 20 см.
В – занурені в землю під кутом 45^0 стальні рейки довжиною 1 м.

13.В пристрої заземлення:
А - можна включати природні заземлювачі;
Б – можна включати металеві оболонки підземних кабелів;
В – не можна використовувати природні заземлювачі.

14.Заземлення ОТЗ слід здійснювати так:
А – від загального контуру заземлення в межах контрольованої території;
Б - від загального контуру заземлення за межами контрольованої території;
В - від часткового контуру заземлення в межах контрольованої території;

15.Екрани кабелів:
А – не повинні мати електричного контакту з іншими металоконструкціями;
Б - повинні мати електричний контакт з металоконструкціями;
В – екрани кабелів повинні з`єдуватись з іншими металоконструкціями черех конденсатор великої ємності;

Контрольна робота №10.

1.Програмові заходи у боротьбі з кіберзлочинністю:
А – шифрування даних при передачі через мережу;
Б – антивірусні програми;
В – забезпечення режиму фізичної охорони об`єктів.

2.Технічні заходи протидії кіберзлочинності включають:
А – охоронну сигналізацію;
Б – резервування особливо важливих комп`ютерних систем;
В – модель порушника.

3. Види доступу до інформації:
А – загальний;
Б – частковий;
В – залежний від повноважень.

4. Правила ефективної роботи дозвільної системи:
А – диференційований підхід до надання доступу з врахуванням класифікованих відомостей;
Б – інтегрований підхід до надання дозволу;
В – документальне закріплення виданого дозволу на право користування тими, або іншими відомостями, що захищаються.

5.Вимоги до системи доступу:
А – чітко розмежувати право керівників різних посадових рівнів в оформленні доступу відповідних категорій виконавців;
Б – система доступу повинна бути модульною;
В – виключати можливість безконтрольної і несанкціонованої видачі документів і виробів будь-кому.

6.Відповідальний за інформаційну безпеку співробітник повинен контролювати:
А – правомірність допуску до таємної інформації співробітників Підприємства;
Б – порядок оформлення на допуск в приміщення КСЗІ;
В – правомірність адресації класифікованих документів з одного підрозділу до іншого.

7.Комплексне застосування всіх заходів захисту інформації в комп`ютерних мережах включає:

А – використання ефективних антивірусних і комп`ютерних засобів;
Б – використанням комп`ютерів не за призначенням.
В – періодична атестація комп`ютерних систем та їх систем захисту.

8. Головна обставина, яка потребує підтвердження при виявленні несанкціонованого доступу:
А – встановлення часу вчинення несанкціонованого доступу;
Б – встановлення інформації, до якої було одержано несанкціонований доступ;
В – виявлення особи, яка вчинила НСД.

9. Факти, які можуть свідчити про підготовку до НСД до комп`ютерної інформації:
А – випадки перезапису окремих даних без серйозних на те підстав;
Б – надмірне зацікавлення окремих співробітників змістом своїх роздруківок;
В – перебування працівників на робочому місці понад встановлений час під приводом здійснення термінових робіт без виникнення такої необхідності.

10. Відомості, які проявляються при несанкціонованому знятті інформації, шляхом копіювання:
А – тимчасова відсутність носіїв інформації чи пристроїв, що містять дані носії;
Б – факт блокування системи протягом більшого проміжку часу, ніж при звичайній роботі доступу до інформації чи іншим пристроям системи, викликані процесами копіювання;
В –зацікавленість до розташування будб-якої інформації в АС.

11.До слідів, що залишаються на магнітних носіях і вказують на сторонній доступ до інформації можливо віднести наступні зміни:
А – перейменування каталогів і файлів;
Б – зміна розмірів і змісту файлів;
В – поява нових каталогів та файлів.

12.На неправомірний доступ до комп`ютерної інформації можуть вказувати зміни в заданій раніше конфігурації комп`ютера, а саме:

А –зміна заставки і кольору екрана при вмиканні комп`ютера;
Б – незмінний порядок взаємодії з периферійним устаткуванням;
В –незмінний колір ерана при вмиканні комп`ютера.

13.При отриманні інформації про знищення інформації необхідно здійснити перевірку:

А – відомості про доступ чи роботу за комп`ютером осіб, в чиї обов`язки не входять такі дії;
Б – факти збоїв у роботі обчислювальної системи, що викликані програмовими і технічними причинами;
В - відомості про доступ чи роботу за комп`ютером осіб, в чиї обов`язки входять такі дії;

14.Слідами перекручення інформації у вигляді збереженої після вчинення комп`ютерного злочину будуть:

А – програмове забезпечення, яке дозволяє здійснювати перекручення інформації в комп`ютерній системі чи носіях інформації підозрюваного;
Б – збережені в комп`ютерах чи на інших носіях інформації в комп’ютерній системі підозрюваного копії програмового забезпечення, що піддавалося впливу, або його модифіковані варіанти.
В – антивірусне програмне забезпечення.

15.Особи, що вчиняють операційні злочини:

А – оператори комп`ютерів;
Б – системні комп`ютерні програмісти;
В – інженери-зв`язківці.

ПЕРЕЛІК НАВЧАЛЬНО-МЕТОДИЧНОЇ ЛІТЕРАТУРИ

1. М.В. Грайворонський, О.М. Новіков Безпека інформаційно-комунікаційних систем. Підручник. Видавнича група BHV, К. 2009. С.18-49; С.62-68; С.78-86.
2. В.Я. Василяк, С.О. Климчук Інформаційна безпека держави. Курс лекцій. Видавничий дім «Скіф». 135 с.
3. В.В. Домарєв, Скворцов С.О. Організація захисту інформації на об`єктах державної та підприємницької діяльності. Навчальний посібник. К.: Видавництво Європейського університету. 2006. 102 с.
4. А.Б. Стоцький, О.І. Тимошенко, А.М. Гуз та інші, за заг. ред. В.С. Сідака Організаційно- правові основи захисту інформації з обмеженим доступом К.: Видавництво Європейського університету. 2006. 232 с.
5. В.С. Сідак, В.Ю. Артемов Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. К.: КНТ. 2007. 160 с.
6. М.М. Зацеркляний, О.Ф. Мельников Основи економічної безпеки. Навчальний посібник. –К.: КНТ, 2007. – 160 с.
7. С.І. Ніколайчук, Д.Й. Никифорчук, О.В. Тихонова, С.В. Шуженко, Я.Ю. Липчей Протидія злочинів, що вчиняються у сфері використання електронно-обчислювальних машин (комп`ютерів), систем і комп`ютерних мереж. Науково-практичний посібник. –К.: КНТ, 2007. – 196 с.
8. Є.К. Пашутинський Інформаційні технології. Нормативна база. –К.: 2005. -500 с.
9. О.К. Шуаібов Практикум з охорони праці. Навчальний посібник. –У.: Видавництво ДВНЗ «УжНУ» «Говерла». 2008. – 279 с.

Навчально-методичний посібник:
Організаційна робота із захисту інформації в інформаційно-комунікаційних системах (практикум).

Автор: **Шуаібов Олександр Камілович**

Навчально-методичний посібник для самостійної роботи студентів

Підписано до друку 2011 р. Формат 60×84/16
Офсетний друк
Умовн. друк. арк. Облік.-вид.арк.
Замовлення
Тираж 100 №

Видавництво УжНУ "Говерла"
м. Ужгород, вул. Капітульна, 18., тел: 3-12-48

Свідотцтво про внесення до державного реєстру видавців, виготавників і розповсюджувачів продукції-