МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

ШУАІБОВ О. К.

ПРАКТИКУМ З ОРГАНІЗАЦІЙНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Навчальний посібник

Ужгород-2013

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

Практикум з організаційно-технічного захисту інформації в інформаційно-комунікаційних системах. Навчальний посібник для самостійної роботи студентів //Шуаібов О. К. - Ужгород, ДВНЗ «УжНУ», «Говерла». **2013**. – 136 с.-Іл.: 30 . - Бібл.: 12 назв. – Укр. мовою. - 2013 р.

Навчальний посібник написано для курсу «**Організаційно-технічне забезпечення систем захисту інформації»**, який вивчається студентами, що спеціалізуються в напрямі захисту інформації. Він містить матеріал до практичних робіт з організаційних і технічних питань захисту інформації в автоматизованих системах, питання модульного котролю а також 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 організаційно-технічного 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 . . 2013 р.

ЗМІСТ

Передмова ..……..……**4**

1. Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС ..……...**6**

2. Вивчення міжнародного стандарту з оцінювання безпеки інформаційних технологій (ISO/IEC 15408) ….……..…**18**

3. Вивчення організаційної роботи служби захисту інформації в автоматизованих системах……..…….**26**

4. Управління безпекою інформаційно-комунікаційних систем…….....**43**

5. Вивчення чинників, що визначають безпечність застосувангня комп`ютерів та егономічного заберпечення робочого місця оператора відеодисплейного терміналу **58**

6. Вивчення основ імовірнісного аналізу безпеки інформаційних систем ……..**75**

7. Вивчення основних елементів захисного екранування фізичного середовища, в якому розташована інформаційно-комунікаційна система …… **..97**

8. Вивчення захисного заземлення пристроїв інформаційно-комунікаційних систем ……..…..**112**

Питання модульних контролів…….....**128**

Перелік навчально-методичної літератури ……..**135**

ПЕРЕДМОВА

Більшість інформації становить певну цінність, тому інформаційні ресурси потребують захисту від різних впливів, які можуть її знизити. Завдання захисту інформації, переважно державних і військових таємниць, було досить актуальним і незмінним на протязі тисячоліть і полягало в забезпеченні 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 часто 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 вісім практичних тем з організаційно-технічної роботи із захисту інформації в інформаційно-комунікаційних системах.

Матеріали 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 програмних 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 безпеки країн **НАТО** і **ЄС**; основних положень документа С-М(2000) 49; базових принципів захисту та ступенів секретності інформації в країнаї Європи;

2. **Необхідна література.**

Стандарти захисту інформації з обмеженим доступом в країнах **НАТО** і **ЄС**.;

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

3.1.Основні теоретичні відомості.

Термінологія.

Зміст наступних термінів з інформаційної безпеки (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**, 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», тобто такі, для яких визначено рівень обмеження доступу і які внесені до відповідних реєстрів, та «некласифіковані», 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. Інституційні принципи, які покликані забезпечити високий рівень інформаційної безпеки:

широта, глибина, централізація, контрольований доступ, персональний контроль.

Сутність захисту інформації **НАТО** з обмеженим доступом полягає у використанні **принципів: уніфікації** рівнів класифікації інформації в **НАТО, 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 та **інституційованого моніторингу** системи забезпечення

захисту інформації з обмеженим доступом в країнах-учасницях **НАТО**.

Сюди ще належить принцип **відповідності** норм захисту інформації з обмеженим доступом у **НАТО** який 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 термінології **НАТО** ще носить назву *потреба знати* 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** означає вимогу мати в кожній державі-члені **НАТО** інституційований національний уповноважений орган або урядове бюро національної безпеки, яке відповідає за інформаційну безпеку та персонал, а також за збір і

реєстрацію відомостей щодо шпигунства та підривної діяльності.

3.3. Ступені секретності.

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

На даний час затверджено наступний порядок, відповідно до якого встановлено наступні 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 державам **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 країнах **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 та адміністративні.

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) та національні уповноважені органи з безпеки **НАТО (NSA)**.

Структура органів безпеки **НАТО** та структура і функції **NOS** наведені на **рис.1.;2.**

Національний уповноважений орган з безпеки інформації зобов'язаний забезпечувати: 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. Він також проводить перевірку благонадійності всіх громадян своєї країни, які за родом своєї діяльності допущені до інформації з обмеженим доступом, розроблення планів захисту інформації у надзвичайних обставинах для запобігання нелегітимного використання інформації з обмеженим доступом.

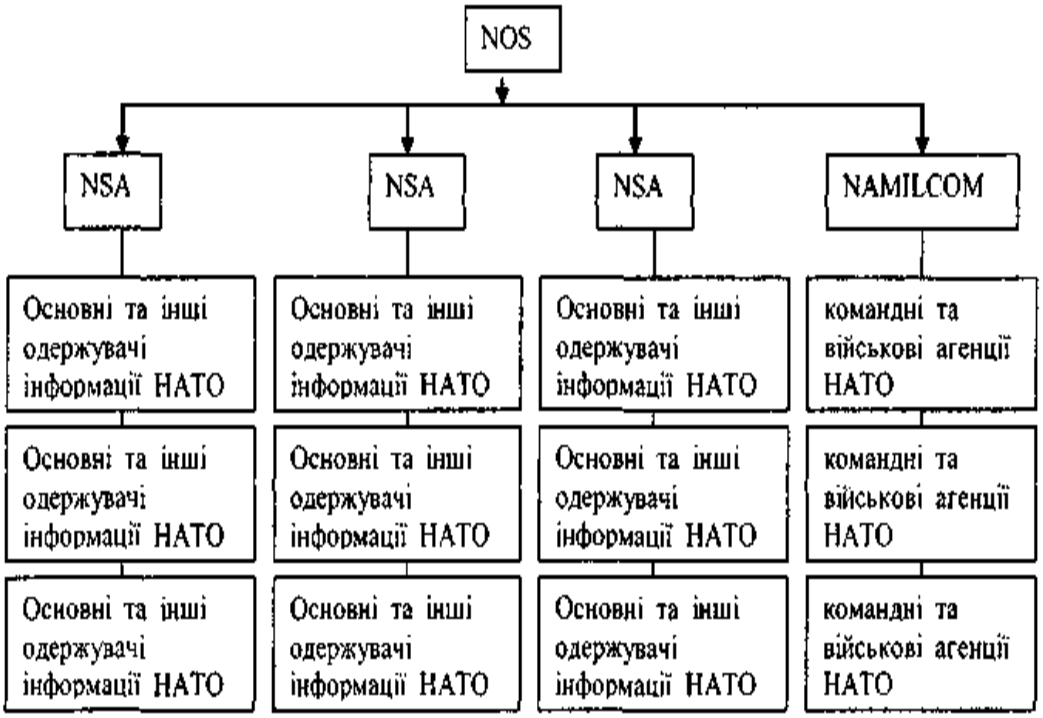


Рис. 1. Органи безпеки **НАТО**.

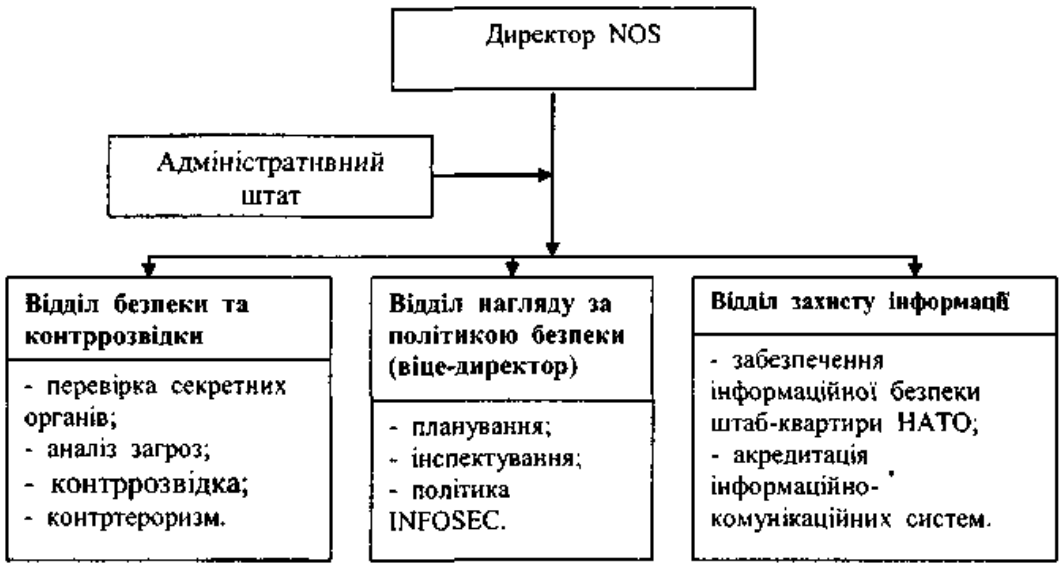


Рис.2. Структура **NOS**.

3.6. Принципи та мінімальні стандарти політики безпеки НАТО.

Базові принципи та мінімальні стандарти політики безпеки **НАТО** стосуються питань створення системи надійних органів безпеки, організації захисту інформації, виробів, територій та споруд та 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, промислова безпека, відповідальність за безпеку, національний орган безпеки, повноважний орган безпеки (DSA); комітет безпеки **НАТО (NSC)**; офіс безпеки **НАТО (NOS)**; військовий комітет **NAMILCOM** та військові організації **НАТО**, а також цивільні організації **НАТО**.

Заходи фізичної безпеки НАТО передбачають захист приміщень та споруд, захист інформації всередині приміщень та споруд, контроль доступу до приміщень та

споруд, захист проти візуального спостереження та прослуховування.

При визначенні того який саме ступінь фізичної безпеки у кожному конкретному випадку необхідний, беруться до уваги наступні чинники: 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 і терористичної або іншої кримінальної діяльності.

У якості заходів забезпечення **фізичної безпеки визначені наступні**: огорожа по периметру та система охоронного освітлення, система виявлення порушника, у тому числі система відеоспостереження, 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 полягають в тому, що особи, яким санкціоновано доступ до інформації з грифом **«Таємно»** і вище, повинні пройти відповідну перевірку на допуск персоналу, що проводиться органом національної безпеки або іншим уповноваженим органом. Процедури видачі сертифіката допуску здійснюються відповідно до політики безпеки **НАТО** і відповідних директив.

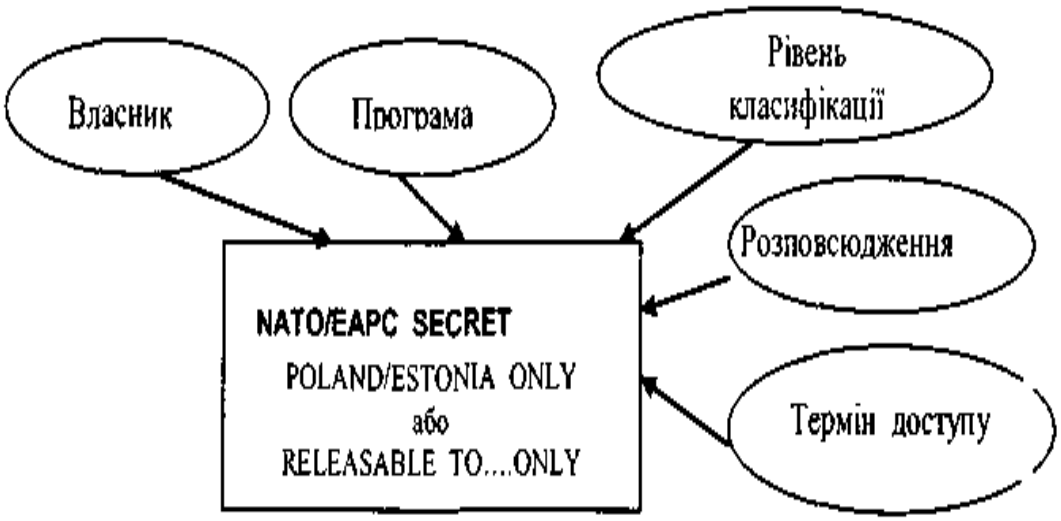


Рис.3. Система маркувань класифікованих документів **НАТО.**

Безпека інформації передбачає нормування таких процедур поводження з документованою інформацією, які виникають при її: маркуванні, класифікації, підготовці та обігу.

3.7. Форми розповсюдження інформації в країнах НАТО.

Існують такі ***форми розповсюдження інформації НАТО***: спорадичне розповсюдження та регулярне 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 до **промислової безпеки** 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** та умови отримання підприємством ліцензій на виробництво продукції та послуг за контрактами **НАТО**. Сюди також належить 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** і процедура 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.

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: «**НАТО**/некласифікована, але чутлива» та «**НАТО**/некласифікована».

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

Згідно з Документом С-М(2002)60, до інформації «**НАТО**/некласифікована» 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. Дайте визначення термінів: «*національна безпека*», «*інформаційна безпека*» та «*організаційно-правові основи інформаційної безпеки*».
2. Наведіть короткий зміст документу С-М (2000) 49.
3. Охарактеризуйте базові принципи, які адекватно відображають сутність захисту інформації, та ступені секретності інформації в країнах **НАТО** і **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 документу С-М(2002)49.
7. Ступені секретності 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 країн **НАТО**.
11. Наведіть структуру документа С-М (2000) 49.
12. Охарактеризуйте задачі, заходи і зони фізичної безпеки в країнах **НАТО**.
13. В чому полягають заходи і процедури безпеки персоналу в країнах **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 в країнах **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 кваліфакаційний аналіз продуктів інформаційних технологій, а також 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 стандарту ISO/IEC 15408.

Основними завданнями з розроблення цього стандарта були: уніфікація національних стандартів у сфері оцінювання безпеки інформаційних технологій (**IT**), підвищення рівня довіри до оцінювання безпеки **IT** та скорочення витрат на оцінювання рівня безпеки **IT** на основі взаємного визнання сертифікатів.

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

Документ **ISO/IEC** 15408 складається з наступних розділів: вступ і загальна модель, функціональні вимоги безпеки і вимоги до забезпечення безпеки.

У документі розглянуто основні аспекти безпеки — забезпечення конфіденційності, цілісності та доступності

інформації та модифікації чи втрати доступу до інформації під час реалізації загроз різного типу.

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 і 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 і користувачам об'єкта оцінювання.

Об'єктом оцінювання називають продукт або систему **ІТ**, яка має ресурси, які 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

Вимоги до безпеки об'єкту оцінювання поділяють на дві категорії: функціональні вимоги, тобто вимоги до тих функцій об'єкту оцінювання, що відповідають за безпеку **ІТ**-продукту та вимоги адекватності, які описують такі властивості об'єкту оцінювання, що 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 IT-продукту та його кваліфікаційний аналіз

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

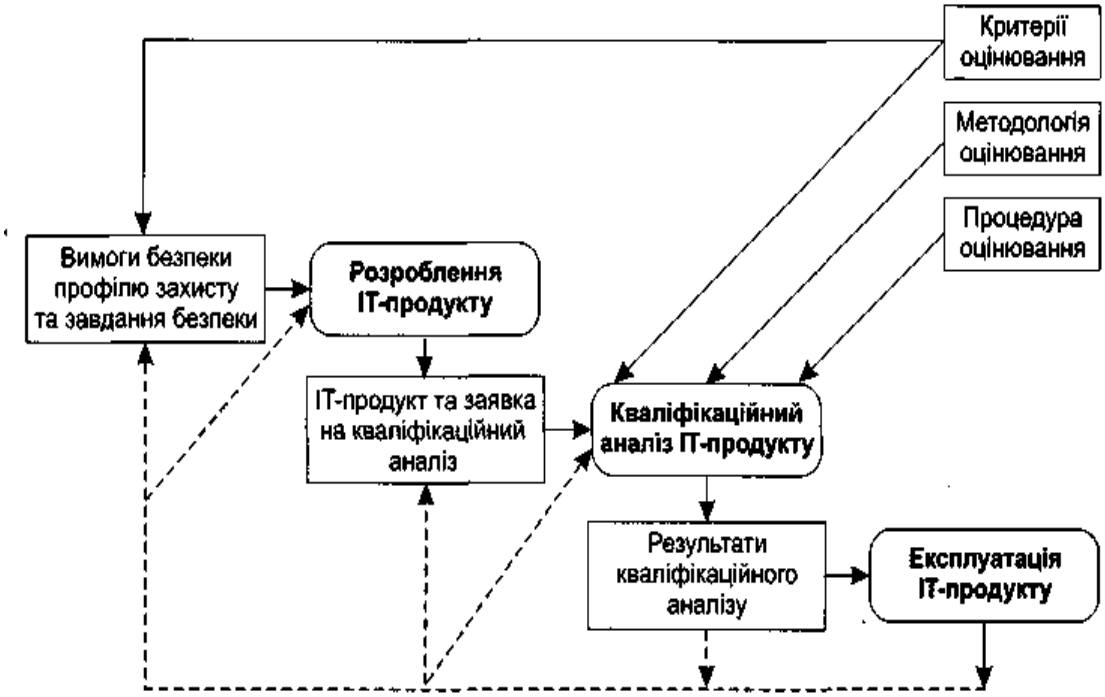


Рис.1. Використання «**Загальних критеріїв**» на етапах існування **ІТ**-продукту.

При кваліфікаційному аналізі **ІТ**-продуктів, окрім «**Загальних критеріїв**» використовують документ «**Загальна методологія**», де подано перелік дій, які необхідно виконати під час оцінювання. Основні принципи, на яких ґрунтується документ «**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'єктів 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; ***розробник***—демонструє об'єкт оцінювання і відповідає за надання відомостей; ***експерт-оцінювач*** - приймає відомості від розробника або

безпосередньо від заявника, здійснює оцінювання об'єктів та надає його результати відповідному органу, а також ***орган оцінювання***— який організовує, підтримує і контролює процес оцінювання. 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**-продуктів здійснюють у кілька етапів. Зокрема, це:

- аналіз профілю захисту на його повноту, несуперечність, а також можливість реалізації та використання як набору вимог до продукту, що аналізують;
- аналіз завдання з безпеки на його відповідність вимогам профілю захисту, а також на повноту, несуперечність, можливість реалізації та використання як опису **ІТ**-продукту;
- 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 і огляд змісту.
2. **Опис об'єктів оцінювання**. Тут подано стислу характеристику об'єктів оцінювання, їх 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'єктів оцінювання, пов'язаних з безпекою: з**агрози безпеці** (опис загроз безпеці, при цьому для кожної загрози вказуються джерело, метод впливу і об'єкт); **політика безпеки** (подається визначення і пояснення правил політики безпеки) та у**мови 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 наступні: задачі захисту, які вирішує сам **ІТ**-продукт; інші задачі захисту.
5. **Вимоги безпеки**. Тут наведено вимоги безпеки, які має задовольняти **ІТ**-продукт для вирішення задач захисту, зокрема це: функціональні вимоги; лише типові вимоги, передбачені у відповідних розділах «**Загальних критеріїв**», які можуть зобов'язувати чи забороняти використовувати конкретні методи та засоби; вимоги адекватності, які є типовими вимогами; вимоги до середовища експлуатації та функціональні вимоги до середовища експлуатації.
6. **Додаткові відомості**. 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 завдання з безпеки. Нижче наведено інформацію про структуру завдання з безпеки та зміст основних розділів.
8. **Вступ.** Тут йдеться про призначення завдання з безпеки, а також подано інформацію, необхідну для ідентифікації завдання. Розділ містить: **ідентифікатор** (унікальне ім'я,

яке використовують для пошуку й ідентифікації завдання з безпеки і відповідного йому ІТ-продукту); **огляд змісту** (приведена анотація завдання з безпеки, ознайомившись із якою споживач зможе дізнатися, чи здатний ІТ-продукт вирішити його задачі); **заявка на відповідність «Загальним критеріям»** (це опис властивостей ІТ-продукту, що підлягають кваліфікаційному аналізу) і **опис ІТ-продукту**.

В описі середовища експлуатації приведено **з**міст підрозділів розділу. Тут також описані загрози безпеці, політика безпеки та умови експлуатації.

9. **Задачі захисту.** Цей розділ збігається з однойменним розділом профілю захисту і включає задачі захисту, що вирішує **ІТ**-продукт та інші задачі захисту.
10. **Вимоги безпеки.** Тут наведено вимоги безпеки, якими керувався розробник **ІТ**-продукту, що дає йому змогу заявляти про успішне вирішення задач захисту.
11. **Загальні специфікації ІТ-продукту**. Приведено відображення реалізації **ІТ**-продуктом вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту. Серед цих специфікацій виокремлюють наступні: **специфікації функцій захисту (**це **о**пис функціональних можливостей засобів захисту **ІТ**-продукту, заявлених розробником як таких, що реалізують вимоги безпеки); **специфікації рівня адекватності** (тут **в**изначається заявлений рівень адекватності захисту ІТ-продукту та його відповідність вимогам адекватності через подання параметрів технології проектування і створення **ІТ**-продукту).
12. **Заявка на відповідність профілю захисту.** Завдання з безпеки претендує на задоволення вимог одного чи кількох профілів захисту, для кожного з яких розділ буде містити таку інформацію.
13. **Обґрунтування.** Тут доводиться, що завдання з безпеки містить повну і зв'язну множину вимог того, 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 стандарту **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 стандарту **ISO/IEC** 15408.
5. Охарактеризуйте застосування «**Загальних критеріїв**» на різних етапах життєвого циклу **IT** – продукту.
6. Що включає процес оцінювання об`єкта за документом «Загальна методологія»?
7. Якими 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 наступних 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 і 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 і 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 і закордонними організаціями;
- дослідження технології оброблення інформації в **АС** задля виявлення найюільш імовірних 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 і експлуатації **КСЗІ**;
- організація навчання персоналу з питань забезпечення захисту інформації.

Під час **створення КСЗІ** служба захисту інформації виконує наступні функції. Вона визначає дані, які підлягають захисту під час їх оброблення, та інші об'єкти захисту в **АС**, виконує класифікацію інформації за вимогами до її конфіденційності або значущості для організації, встановлює необхідні рівнів захищеності інформації і порядок введення (виведення) інформації та її використання. **КСЗІ** розробляє і коригує моделі загроз, моделі захисту інформації та політики безпеки інформації в **АС**; організовує і координує заходи із проектування і розроблення **КСЗІ**, приймає безпосередню участь у проектуванні **КСЗІ**; здійснює підготовку технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення **КСЗІ**; організовує заходи і приймає участь у випробуваннях **КСЗІ** і проведенні її експертизи. **СЗІ** здійснює також 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**; приймає 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**, а також бере участь у розробленні нормативних документів, чинних у межах організації і **АС**, які встановлюють правила доступу користувачів до ресурсів **АС**, визначають порядок, норми, правила із захисту інформації та здійснення контролю за їх дотриманням.

Під час **експлуатації КСЗІ** служба захисту інформації виконує наступні функції, зокрема, організує процес управління **КСЗІ**; проводить розслідування випадків порушення політики безпеки, небезпечних та непередбачуваних подій, аналіз подій, що спричинили ці порушення, здійснює супроводу банку даних таких подій; проводить заходи у разі виявлення спроб **НСД** до ресурсів **АС,** порушення правил експлуатації засобів захисту інформації чи інших дестабілізуючих факторів; забезпечує контроль цілісності засобів захисту інформації та можливості швидкого реагування на їх вихід із ладу чи порушення режимів функціонування; організовує управління доступом до ресурсів **АС;** здійснює супроводження й актуалізацію баз даних захисту інформації. Служба захисту інформації здійснює також спостереження за функціонуванням **КСЗІ** та її компонентів; підготовку пропозицій відносно удосконалення порядку забезпечення захисту інформації в **АС**, впровадження нових технологій захисту і модернізації **КСЗІ**; організацію та проведення заходів із модернізації, тестування, оперативного відновлення функціонування **КСЗІ** після збоїв, відмов, аварій **АС** або **КСЗІ**; примає участь у заходах із модернізації **АС**; забезпечеє супроводження і актуалізацію еталонних, архівних і резервних копій

програмних компонентів **КСЗІ** та їх зберігання і тестування; здійснює аналітичне оцінювання поточного стану безпеки інформації в **АС**; проводить інформування власників інформації про технічні можливості захисту інформації в **АС** і встановлені для персоналу і користувачів **АС** типові правила. Важливою задачею **СЗІ** є 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 **АС** про виконання користувачами **АС** вимог із захисту інформації; аналіз відомостей про технічні засоби захисту інформації нового покоління та обґрунтування пропозицій із придбання таких засобів; здійснення контролю за виконанням персоналом і користувачами **АС** вимог, норм, правил, інструкцій із захисту інформації відповідно до визначеної політики безпеки інформації; здійснення контролю за забезпеченням охорони і порядку зберігання документів, які містять відомості, що підлягають захисту; розроблення та реалізація спільно з **РСО** комплексних заходів із забезпечення безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, 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**, а також спеціальні програми навчання з урахуванням особливостей технології оброблення інформації в організації (**АС**); організовують та проводять навчання користувачів і персоналу **АС** правилам роботи з **КСЗІ** та захищеними технологіями і ресурсами; узгоджують навчальні плани і плани з підвищення кваліфікації з державними органами та іншими організаціями; забезпечують навчальний процес необхідною матеріальною базою.

3.3. Права й обов'язки служби захисту інформації

Служба захисту інформації має право:

- ♦ здійснювати контроль за діяльністю будь-якого структурного підрозділу організації щодо виконання ним вимог нормативних актів та документів із захисту інформації;
- ♦ пропонувати керівництву організації призупиняти процес оброблення інформації, забороняти його, змінювати режими оброблення у разі виявлення порушень політики безпеки чи виникнення реальної загрози безпеці;
- ♦ складати і надавати керівництву організації акти виявлених порушень політики безпеки, готувати рекомендації щодо їх усунення, а також здійснювати службові розслідування при виявленні порушень;
- ♦ отримувати доступ до документів структурних підрозділів організації, необхідних для оцінювання ефективності вжитих заходів із захисту інформації та підготовки пропозицій щодо подальшого їх удосконалення;
- ♦ вносити пропозиції щодо залучення до проведення заходів із захисту інформації інших організацій, які мають ліцензії на відповідний рід діяльності та навати пропозиції із забезпечення **АС** технічними і програмовими 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 та узгоджувати умови додавання до **АС** нових компонентів, надавати керівництву пропозиції щодо заборони їх використання, якщо вони порушують прийняту політику безпеки;
- ♦ 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,** також давати керівництву організації пропозиції, пов`язані із

узгодженням планів і регламенту відвідування **АС** сторонніми особами.

Служба захисту інформації повинна виконувати наступні 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** правил, інструкцій щодо оброблення інформації, здійснювати контроль за виконанням цих вимог; здійснювати контрольні перевірки стану захищеності інформації; забезпечувати конфіденційність заходів із монтажу, експлуатації та технічного обслуговування засобів захисту інформації; сприяти і брати участь у проведенні вищими органами перевірок стану захищеності інформації в **АС**. **СЗІ** також має сприяти створенню і дотриманню умов зберігання інформації, отриманої організацією на договірних або контрактних 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** та про дотримання встановленого порядку і правил захисту інформації і негайно повідомляти керівництво 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; 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 заходах із захисту інформації; координувати плани діяльності підрозділів та служб організації з питань захисту інформації. Він організовує

навчання співробітників, користувачів та персоналу **АС** щодо питань захисту інформації і повинен особисто виконувати 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**; якість та правомірність документального оформлення результатів робіт окремих етапів створення **КСЗІ** і результатів перевірок.

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

Служба захисту інформації здійснює свою діяльність у взаємодії з різними 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; 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, який відповідає за забезпечення безпеки інформації, або є структурною одиницею підрозділу **ТЗІ**. 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. 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** — 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. До складу **СЗІ** можуть входити різні за фахом спеціалісти, зокрема це: 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 та спеціалісти служби захисту. Змінити структуру **СЗІ** можна лише на підставі рішення, прийнятого на загальних зборах акціонерів або керівництвом організації та затвердженого наказом 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 СЗІ: календарний план заходів із проектування, реалізації, оцінювання, впровадження, технічного обслуговування і експлуатації **КСЗІ;** план заходів із оперативного реагування на непередбачувані ситуації 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.*

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 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; опис компонентів **АС** та технології оброблення інформації; загрози для інформації в **АС**; політика безпеки інформації; система документів із забезпечення захисту інформації в АС.

4.1. Завдання захисту інформації в АС

До **завдань захисту** інформації в **АС** належать: ефективне знешкодження загроз ресурсам **АС**; забезпечення визначених політикою безпеки властивостей інформації під

час створення та експлуатації **АС**; своєчасне виявлення та знешкодження загроз ресурсам **АС**, причин і умов виникнення порушень функціонування **АС** та її розвитку; створення механізму та умов оперативного реагування на загрози безпеці інформації та 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**. Важливим є і 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 дії фізичних та юридичних осіб, 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; 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; засоби і системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту та засоби захисту користувачів АС, власників інформації і АС, а також їхніх прав.

Безпеку інформації в АС забезпечують шляхом: організації та впровадження системи допуску співробітників до інформації, яка потребує захисту; організації обліку, зберігання, обігу інформації та її носіїв; організації та координації робіт із захисту інформації, яка обробляється та

передається засобами **АС**; здійснення контролю за забезпеченням захисту інформації, і за збереженням конфіденційних документів.

4.2. Класифікація інформації, що обробляють в АС

Класифікація інформації дає змогу її власнику або власнику автоматизованої системи визначити методи і способи захисту даних кожного окремого типу. Всі дані в **АС** класифікують за режимом доступу, правовим режимом та 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 великої шкоди. З метою встановлення правил доступу 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, периферійні пристрої; програмне забезпечення та дані тимчасового і постійного зберігання.

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** доцільно розробити схему інформаційних потоків, указавши для кожного елементу 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 і профілактичні заходи, а також інженерно-технічні заходи і 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 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 змінення умов; 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** та перегляд результатів виконання затверджених заходів і робіт із захисту інформації.

До контрольно-правових заходів, зокрема, належать: контроль за виконанням персоналом 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 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 встановленим правилам безпеки інформації, новим методам захисту інформації, а також із підвищення їхньої кваліфікації.

Навчання здійснюють згідно з програмою, затвердженою керівництвом організації чи **АС**. Навчальні програми повинні 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.

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 про роботу **СЗІ.**
3. Охарактеризуйте статус служби захисту інформації (**СЗІ)**.
4. Яка 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 із забезпечення 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 політикою 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?

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».

3.1. Структура й основний зміст стандарту

Документ складається з передмови, вступу та 15 - ти розділів, зокрема, це: вступ, сфера застосування, терміни та визначення, структура стандарту, оцінювання і оброблення ризиків, політика безпеки, організація забезпечення безпеки інформації, управляння ресурсами, безпека персоналу, фізична безпека і безпека середовища, придбання,

розроблення та супроводження інформаційних систем. Сюди належать і розділи з управління: комунікаціями і операціями, доступом, інцидентами безпеки, безперебійністю бізнесу та дотриманням вимог.

У вступі розлянуто наступні питання: що являє собою 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 пункти вступу більш детально.

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

Пункт «**Як затвердити вимоги до безпеки**» включає три базові джерела вимог до системи безпеки організації:

- специфічні ризики порушення безпеки, які загрожують ресурсам організації і для яких оцінюють уразливість та імовірність 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 пункті «**Визначення ризиків безпеки**» відзначають важливість відповідності між цінністю інформаційних ресурсів організації та витратами на систему їх захисту.

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

У пункті «**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 і підтримка безперебійної роботи, а також управління інцидентами безпеки інформації.

У пункті «**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. Сюди також належать положення про: 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 та упровадження системи показників, призначеної для оцінювання ефективності управління безпекою інформації.

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

Сфера застосування (п.1). У цьому пункті надано інформацію щодо призначення стандарту, містяться рекомендації і загальні принципи з ініціювання,

впровадження, супроводження й удосконалення управління безпекою інформації в організації.

Терміни та визначення (п.2). 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 (п.3). Тут наведеноно структуру стандарту де сформульовано 39- ть цілей управління, досягнення яких забезпечує захист інформаційних ресурсів. Опис цілей керування фактично містить специфікації функціональних вимог до архітектури управління безпекою інформації організації. Для кожної із цілей керування названо засоби керування.

Оцінювання й оброблення ризиків (п.4). У пункті показано відповідність між цінністю інформаційних ресурсів організації та витратами на систему захисту інформації. Для визначення витрат на систему захисту повинні враховуватись рівень ризику та збитки, яких може бути завдано організації. Ризики мають зумовлювати належні пріоритети і дії керівництва щодо управління безпекою інформації та впровадження відповідних засобів захисту.

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. Основні 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, а також 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 (п.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. В даному розділі рекомендовано наступний зміст цього документу: 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, політика забезпечення безперебійної роботи організації; визначення загальних і конкретних обов'язків із забезпечення режиму безпеки інформації і 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 (п.6). У цьому пункті визначено цілі управління в таких підрозділах, які пов`язані інфраструктурою безпеки інформації організації та питаннями безпеки доступу сторонніх організацій.

Управління ресурсами (п.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 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 (п.8). Тут наведено питання 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 пункт містить такі положення.

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, 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 (п.9). У пункті розглянуто заходи з створення та адміністрування зон безпеки і контрольованих периметрів, а також заходи 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 цілі управління в таких підрозділах.

1. **Зони безпеки**. Мета заходів з адміністрування зон безпеки полягає у запобіганні 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**. Метою заходів з організації захисту обладнання є запобігння втратам, 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 та необхідності безпечної утилізації обладнання і носіїв інформації.

Управління комунікаціями й операціями (п.10). Пункт 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.

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.

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.

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.

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 (п.11). Даний пункт присвячено розгляду питань контролю за логічним доступом до комп'ютерних систем і даних, що дає змогу запобігати несанкціонованому доступу. У розділі сформульовано сім цілей управління у наступних 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.

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 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.

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 (п.12). Цей пункт 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. В цьому пункті наведено шість підпунктів.

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.
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 (п.13). Даний пункт присвячено питанням виявлення подій, що впливають на безпеку інформації, та слабких місць у системі безпеки задля гарантування можливості вживати своєчасних заходів протидії. Закрему тут розглянуто питання: повідомлення про інциденти безпеки інформації та слабкі місця та управління інцидентами безпеки інформації та удосконаленнями.

Управління безперебійністю бізнесу (п.14). Пункт 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 (п.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 аудиту 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, яку ще називають системою управління інформаційною безпекою. **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.

4. Завдання лабораторної роботи.

4.1. Виконати аналіз змісту стандарту 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. Охарактеризуйте структуру і основний зміст стандарту **ISO/IEC 15408**.
2. Які питання безпеки інформації висвітлено у вступі до цього стандарту ?
3. В чому полягають необхідні заходи і засоби для створення системи безпеки інформації за стандартом **ISO/IEC 15408?**
4. Сфера застосування статдарту **ISO/IEC 15408**.
5. Оцінювання і оброблення ризиків. Можливі варіанти оброблення ризиків.
6. Охарактеризуйте політику безпеки згідно стандарту **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.

ТЕМА-5. ВИВЧЕННЯ ЧИННИКІВ, ЩО ВИЗНАЧАЮТЬ БЕЗПЕЧНІСТЬ ЗАСТОСУВАННЯ КОМП`ЮТЕРІВ ТА ЕРГОНОМІЧНОГО ЗАБЕЗПЕЧЕННЯ РОБОЧОГО МІСЦЯ ОПЕРАТОРА ВІДЕОДИСПЛЕЙНОГО ТЕРМІНАЛУ

1. **Мета роботи.**

Ознайомлення з технікою безпеки роботи та ергономічними вимогами до робочого місця оператора відеодисплейного терміналу (**ВДТ**). Засвоєння методики організації робочого місця оператора **ВДТ** з урахуванням ергономічних вимог.

2. **Необхідні матеріали.**

Шуаібов О.К. // «Практикум з охорони праці». Навчальний посібник. 2008. Вид. УжНУ «Говерла». 279 с.

Сачков Л.С., Медвідь М.К. “Охорона праці (законодавчі та нормативні акти, порядок реалізації та коментарі до них). Київ.: АТ “ОКО”, 1995. 390 с.

Охорона праці в Україні. Нормативна база // упорядник Роїна О.М. К. КНТ. 2006. 420 с.

3. **Основні теоретичні відомості.**

Основні терміни : Інформаційні системи, ергономіка, дисплей, антропометричні дані, клавіатура, санітарно-гігієнічні умови праці оператора **ВДТ**, статичні і динамічні антропометричні характеристики, перцентиль, середньоквадратичне відхилення, математичне очікування, середнє арифметичне значення, зона моторного поля оператора **ВДТ**, манекен, параметри ергономічної оцінки організації діяльності оператора **ВДТ**.

4.1. Організація робочого місця оператора ВДТ відповідно до антропометричних характеристик

У зв'язку з широким використанням дисплеїв у автоматизованих системах управління, інформаційних

системах та системах передачі даних з'явився цілий комплекс ергономічних проблем. Дисплей має відповідати структурі і процесу діяльності людини, а в його конструкції повинні враховуватися антропометричні, біомеханічні і психологічні можливості людини.

Ергономічні вимоги, які пред'являються до дисплеїв, розрізняють залежно від конкретних типів і завдань, що на них виконуються.

Робоче місце оператора - частина простору в системі «людина - машина» (**СЛМ**), оснащена засобами відображення інформації, органами управління і допоміжним обладнанням і призначена для здійснення діяльності оператора **СЛМ**.

Забезпечення організації робочого місця оператора за дисплеєм передбачає організацію робочого місця відповідно до антропометричних характеристик (**АХ**); виконання ергономічних вимог до розміщення технічних засобів на робочому місці; до світло- і кольоро-технічних характеристик дисплеїв, до літерно-цифрової інформації дисплеїв, клавіатури; необхідні санітарно-гігієнічні умови праці.

Антропометричні характеристики поділяються на динамічні і статичні (рис.1) .

Динамічні антропометричні характеристики використовують для визначення обсягу робочих рухів, зон досяжності й огляду, за ними розраховують просторову організацію робочого місця, розмах рухів обертових і селекторних перемикачів, біомеханічні моделі людини й манекена.

До **статичних** антропометричних характеристик належать розміри, виміряні в статичному положенні людини, яка зберігає при вимірах одну й ту саму позу.

Умовність і постійність пози забезпечують ідентичність умов вимірів. Статичні антропометричні характеристики використовують для встановлення розмірів конструктивних параметрів робочого місця або виробу, використання діапазону вимірів у випадку їх регулювання, а також при

проведенні ергономічної експертизи і конструюванні манекенів.

Особливу групу статичних антропометричних характеристик складають габаритні розміри тіла, тобто його найбільші розміри в різних положеннях і позах, орієнтовані в різних площинах.

Правила використання антропометричних характеристик:

- визначити групу населення, для якої буде призначене проектоване чи організоване робоче місце ;
- вибрати групу антропометричних характеристик, що є основою для визначення розміру конструкції устаткування;
- установити, якому відсотку працюючих має задовольняти певне робоче місце (устаткування) і за допомогою перцентилів (**перцентиль** - сота частка вимірюваної сукупності, що виражається у відсотках і якій відповідає визначена величина відповідної антропометричної характеристики) або часткою σ знайти відповідне йому значення антропометричних характеристик;
- урахувати відповідно поправки на одяг і взуття.

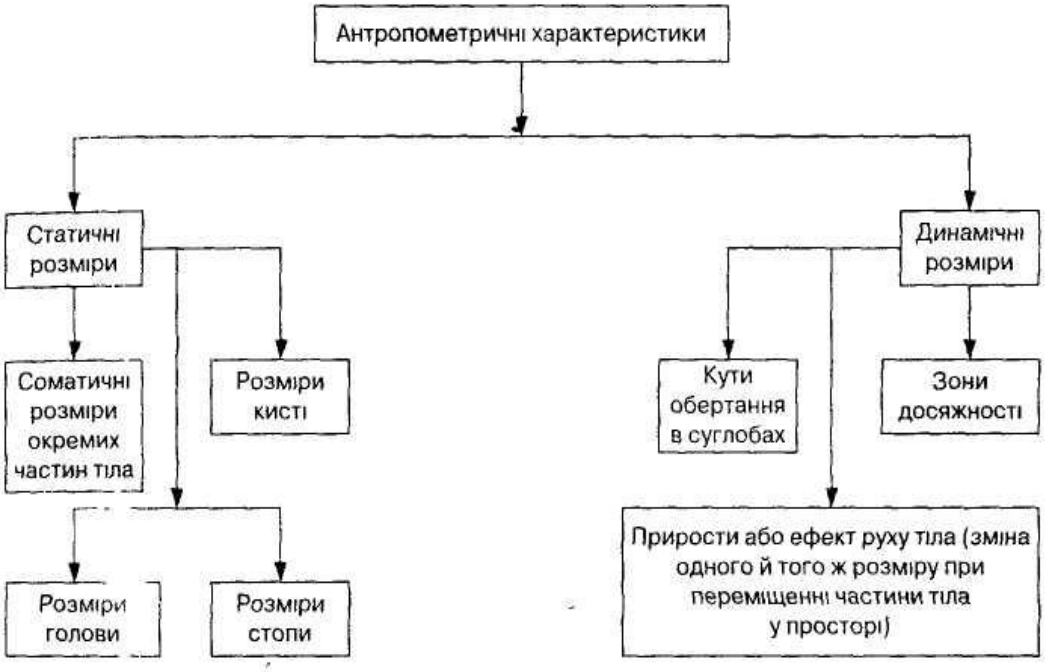
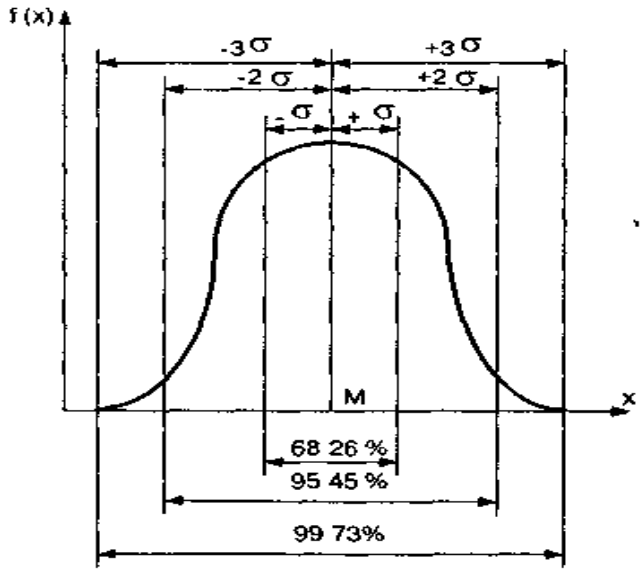


Рис.1. Класифікація антропометричних характеристик.

При визначенні контингенту людей необхідно враховувати вікову, статеву і національну належність. Вікові розбіжності ґрунтуються на біологічних особливостях різних стадій індивідуального розвитку. При визначенні ергономічних завдань орієнтуються на усереднені антропометричні характеристики дорослого населення країни.

При проектуванні робочого місця слід звертати увагу також на національно зумовлені антропометричні характеристики.

При ергономічному забезпеченні організації робочого місця оператора за дисплеєм варто знати, що воно має відповідати антропометричним характеристикам, які визначають розміри тіла і його окремих частин.



Антропометричні характеристики є випадковими величинами, які підлягають нормальному закону розподілу (рис.2). Необхідний діапазон мінливості досліджуваної антропометричної характеристики задається або за середньоквадратичним відхиленням **σ** (а) стосовно математичного очікування (**M**), або за допомогою перцентилів (співвідношення між ними наведено в табл.1).

Рис.2. Крива нормального розподілу.

Таблиця 1.

Вихідні дані для вибору діапазону вимірів антропометричних характеристик

Інтервал, M±nσ	Перцентиль, %	Кількість людей, антропометричні характеристики яких вміщуються в інтервалі,
M±2,5σ	1-99	98
M±2,0σ	2,5 - 97,5	95
M+1,65σ	5-95	90
M±1,15σ	12,5-87,5	75
M±σ	16-84	68
M±0,67σ	25-75	50

Варіативність багатьох характеристик людей, тобто відхилення при антропометричних вимірах тіла людини, наближається до цього закону розподілу: більшість вимірів величин лежить у центрі кривої і тільки незначна частина - по краях. При обліку антропометричних характеристик необхідно використовувати дані кривої при розрахунку довірчого інтервалу.

Основною характеристикою кривої розподілу є середнє арифметичне значення **M**, яке є часткою від ділення Σx на **N**, де ***x*** - величина виміру, **N** - кількість вимірів. Іншою характеристикою є середнє квадратичне відхилення σ:

$$\sigma = \sqrt{\frac{\sum (x - M)^2}{N}}, \qquad (1)$$

При ідеальному дотриманні закону нормального розподілу діапазон величин в інтервалі значень **σ** від -1 до +1 вміщує 68% вимірів характеристик. При проектуванні, так і при оцінці експлуатованих **СЛМ** переважне значення має впровадження пристроїв, які дають змогу регулювати робоче місце відповідно до розмірів тіла людини.

4.2. Методика організації робочого місця оператора за дисплеєм відповідно до антропометричних характеристик

Робоче місце повинно бути містким для оператора з максимальними розмірами тіла і досяжним для оператора з мінімальними розмірами заданого контингенту.

При організації робочого місця враховують антропометричні характеристики жінок (якщо працюють тільки жінки) і чоловіків (якщо працюють лише чоловіки); якщо робоче місце розраховане для чоловіків і жінок - показники жінок і чоловіків.

Перевірка відповідності параметрів робочого місця (висота робочої поверхні, її розміри; висота сидіння крісла, простору для ніг, підставки для ніг тощо) антропометричним характеристикам операторів здійснюється за допомогою площинних манекенів.

Спочатку знаходять значення антропометричних характеристик для заданого контингенту операторів за табл. 2 і 3, в яких наведені дані чоловіків і жінок, що виконують роботу сидячи або стоячи, для п'яти перцентилів трьох груп населення:

А - населення з малими значеннями повздовжніх ознак;

Б - населення з середніми значеннями повздовжніх ознак;

В - населення з великими значеннями поздовжніх ознак.

Потім необхідно урахувати поправку на одяг і взуття (табл.4). Після вибору антропометричних характеристик операторів для робочої пози сидячи і внесення поправок на одяг і взуття будують два площинних манекени в масштабі 1:10 за мінімальними і максимальними антропометричними характеристиками. Манекени виготовляють із цупкого матеріалу - картону, ватману й ін. У шарнірних з'єднаннях частин манекена (на рис.3 показані точками) використовують мідний дріт діаметром 0.4-0.5 мм. За даними розрахунку і рекомендованій ширині вирізають із цупкого матеріалу прямокутні частини манекена (табл.5).

Таблиця 2

Статичні антропометричні характеристики в положенні сидячи

Найменування ознаки	Група населення	Значення ознаки, відповідне перцентилям (см)									
		для чоловіків					для жінок				
		1	5	50	95	99	1	5	50	95	99
1	2	3	4	5	6	7	8	9	10	11	12
Висота (розмір 1) верхівкової точки над сидінням (22)*	А	82,20	84,00	88,60	93,10	95,00	76,80	76,80	82,90	87,30	89,00
	Б	84,00	85,90	90,50	95,00	99,00	79,30	81,20	85,60	90,00	91,80
	В	85,40	87,30	91,90	96,60	98,50	81,50	83,30	87,60	92,00	93,80
Висота (розмір 2) очей над сидінням (24)*	А	68,20	70,20	74,90	79,70	81,60	63,80	65,90	70,90	76,00	78,10
	Б	70,50	73,10	77,40	81,80	84,40	67,20	69,00	73,40	77,80	79,60
	В	71,90	74,00	78,90	83,80	85,90	69,90	71,60	76,70	79,80	81,50
Висота (розмір 3) плеча над сидінням (25)	А	53,80	55,60	59,97	64,30	66,10	50,10	51,80	55,80	59,80	61,40
	Б	53,20	55,20	59,96	64,70	66,60	50,80	52,50	56,60	60,70	62,40
	В	54,80	56,70	61,30	65,90	67,80	52,80	51,50	58,60	62,80	64,50
Висота (розмір 4) ліктя над сидінням (26)*	А	17,50	18,95	22,40	25,96	27,40	16,60	18,20	22,10	25,90	27,50
	Б	17,00	18,70	22,86	27,10	28,80	16,60	18,25	22,20	26,00	27,70
	В	17,50	19,10	22,86	26,50	28,10	17,94	19,30	22,50	25,70	27,10
Висота (розмір 5) коліна над підлогою (26)*	А	47,40	48,90	52,54	56,18	57,69	43,85	45,21	48,49	51,78	53,14
	Б	50,13	51,99	56,47	60,93	62,79	57,14	48,57	52,02	55,47	56,90
	В	50,06	51,70	55,64	59,59	61,23	46,74	48,10	51,37	54,65	56,01
Ліктьова —	А	41,98	43,31	46,50	49,70	51,02	38,60	39,76	42,57	45,37	46,54

пальцьова Ш точка (розмір 6) — горизонтальна відстань від вершини ліктьового відростка ліктьової кістки до пальцьової третьої точки (34)*	Б	42,30	43,99	48,07	52,15	53,84	39,94	41,09	43,87	46,65	47,80
	В	42,76	44,23	47,65	51,03	52,51	40,12	41,18	43,74	46,29	47,35
Горизонтальна відстань (розмір 7) від спинки до точки надколінної чашки, яка найбільше виступає вперед (38)*	А	50,75	53,18	59,04	64,90	67,33	49,24	51,30	56,29	61,29	63,34
	Б	53,03	55,33	60,89	66,45	68,75	51,05	53,02	57,63	62,52	64,49
	В	55,17	56,87	60,79	64,70	66,40	50,65	52,41	56,67	60,93	62,70
Довжина (розмір 8) стопи (41)*	А	23,52	24,26	26,04	27,81	28,55	21,22	21,99	23,85	25,70	26,47
	Б	23,88	24,71	26,72	28,72	29,55	21,35	22,13	24,63	25,92	26,70
	В	24,33	25,12	27,03	28,93	29,72	22,38	23,04	24,62	26,19	26,85
Найбільший поперечний розмір тіла — горизонтальна відстань між точками зовнішньої поверхні виступають у сторону (17)*	А	41,84	43,82	48,37	52,92	54,89	38,39	40,75	46,44	52,14	54,49
	Б	42,90	44,85	49,55	54,25	56,20	39,77	41,87	46,65	51,52	53,53
	В	42,94	44,64	48,55	52,47	54,17	40,77	42,38	46,27	50,15	51,76

У дужках указано номер антропометричної ознаки за Держстандартом від 12.02.2004.

Таблиця 3

Статичні антропометричні характеристики оператора **ВДТ** в положенні стоячи

Найменування ознаки	Група населення	Значення ознаки, відповідне перцентилям (см)									
		Для чоловіків					Для жінок				
		1	5	50	95	99	1	5	50	95	99
Висота верхівкової точки над підлогою (довжина тіла, зріст (I))*	А	155,70	159,30	167,70	176,06	179,70	144,40	147,40	155,40	163,40	166,50
	Б	157,70	161,40	172,30	183,20	186,55	147,30	150,80	159,50	168,00	171,60
	В	163,30	167,21	176,50	186,40	190,30	153.70	157,00	165,10	173,10	176,50
Висота ока над підлогою (2)*	А	143,40	146,70	154,80	162,82	166,10	132,10	135,40	143,40	151,40	154,70
	Б	145,60	149,30	159,70	170,60	174,30	135,80	139,40	147,80	156,20	159,70
	В	150,30	154,30	164,00	173,80	177,80	142,20	145,60	153,60	161,60	164,90
Висота плеча над підлогою (3)*	А	128,00	131,20	139,10	147,60	150,20	117,10	120,30	128,60	135,70	138,80
	Б	128,40	132,60	142,80	153,00	157,20	120,20	123,70	131,80	140,30	143,70
	В	133,40	137,20	146,10	155,60	159,00	125,60	128,70	136,30	143,90	147,10
Найбільший поздовжній діаметр тіла (17)*	А	41,80	43,80	48,40	52,90	54,90	38,40	40,80	46,40	52,10	54,50
	Б	42,90	44,85	49,60	54,25	56,20	39,80	41,80	46,60	51,50	53,50
	В	42,94	44,64	48,55	52,47	54,20	40,80	42,40	46,30	\50,20	51,80
Передня досяжність руки (19)	А	75,90	78,73	84,60	90,70	93,20	68.40	70,70	76,10	81,50	83,80
	Б	73,60	76,70	84,23	91,73	94,84	68,70	71,20	77,10	83,10	85,50

	В	75,30	78,10	84,83	91,60	94,34	69,80	72,00	77,50	83,00	85,30
Передня максимальна досяжність руки (20)	А				—	—	—	—	—	—	—
	Б	119,80	124,10	134,50	144,90	149,20	114,00	117,70	126,70	135,40	139,10
	В	—	—	—	—	—	—	—	—	—	—
Вертикальна досяжність руки (21)*	А	198,30	203,40	215,80	228,21	233,30	179,80	184,70	196,70	208,60	213,50
	Б	—	—	—	—	—	—	—	—	—	—
	В	206,70	212,30	225,90	239,60	245,20	193,20	197,90	209,20	220,50	225,20

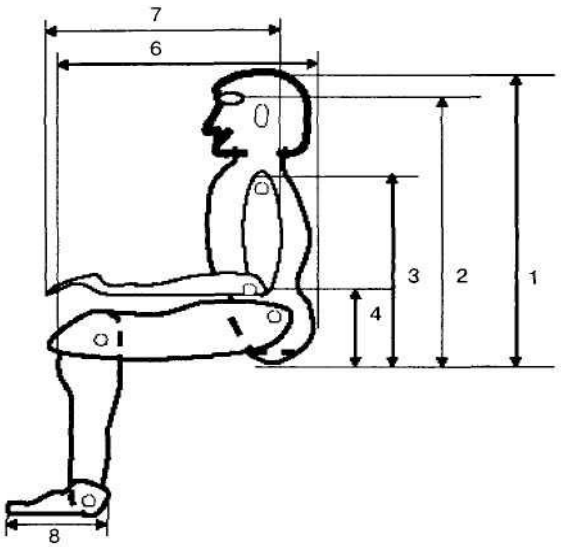


Рис.3. Основні розміри площинного манекена

Таблиця 4

Поправки на одяг і взуття

Ознака	**Величина поправки, мм**
Висота плеча над сидінням (3)*	5,0
Довжина плеча (3 — 4)**	5,0
Довжина передпліччя і кисті (6)	5,0
Довжина стегна (7)*	5,0
Висота коліна (5)*	25,0
Довжина стопи (8)*	30,0

Таблиця 5

Рекомендована ширина прямокутників частин манекена, мм.

(1) «тулуб»	20-30
(2)«плече»	10
(3) «передпліччя» і «кисть»	7
(4)«стегно»	15
(5) «гомілка»	12
(6)«стопа»	7

При вирізанні прямокутників «плече», «передпліччя» і «кисть» необхідно збільшити їх розміри відносно розрахованих для кріплення до «тулуба» і один до одного, з тим, щоб витримати розрахункові розміри при складанні манекена. Після збирання частин манекена прямокутникам надають форми, близької до прототипу.

Після виготовлення плоских манекенів будують ескіз робочого місця оператора для робочої пози сидячи, який би відповідно розмірам тіла (місткість для оператора з максимальними розмірами тіла і досяжність для оператора з мінімальними розмірами).

Для цього на чистому аркуші паперу поміщають манекен з максимальними антропометричними характеристиками, надають йому фізіологічно раціональну робочу позу, тобто позу, що відповідає критеріям функціонального комфорту: випрямлене положення хребетного стовпа зі збереженням його природних вигинів, мінімальне навантаження на м'язову систему тіла людини; відсутність хворобливих відчуттів у результаті дії елементів робочого місця на тіло людини, яка сидить:

- відстань від очей оператора до дисплея 500 - 700 мм;
- природний нахил корпуса вперед на 5° - 10°;
- кут згинання між стегном і гомілкою 95° - 135°;
- ступня на підлозі;
- стегно горизонтальне;
- оператор максимальних розмірів не повинен

упиратися ступнею в стійку столу або підставки;

- оператор повинен мати можливість опиратися ліктем на робочу поверхню і працювати з документами;
- відстань від сидіння крісла до нижнього краю робочої поверхні не менше 150 мм.

Після того, як манекену надали фізіологічно раціональну робочу позу сидячи, потрібно намалювати контури робочого столу, на якому розташувати дисплей, визначити кут огляду, висоту робочої поверхні, сидіння крісла. Потім до цього рисунка необхідно прикласти манекен, виготовлений за мінімальними антропометричними характеристиками у фізіологічно раціональній робочій позі сидячи. Перевірити зручність робочого місця (висоту робочої поверхні, зони досяжності моторного поля й ін..

Моторне поле робочого місця оператора СЛМ – це частина робочого місця оператора, в якому розташовані органи управління, які використовує оператор, і здійснюються його рухові дії з управління **СЛМ**.

Розрізняють зону досяжності, зону легкої досяжності та оптимальну зону досяжності моторного поля.

Зона досяжності моторного поля робочого місця оператора - частина робочого місця оператора, обмежена дугами, які описуються максимально витягнутими руками при русі їх у плечовому суглобі.

Зона легкої досяжності моторного поля робочого місця оператора - частина моторного поля робочого місця оператора, обмежена дугами, які описуються розслабленими руками при русі їх у плечовому суглобі.

Оптимальна зона моторного поля робочого місця оператора - частина моторного поля робочого місця оператора, обмежена дугами, які описуються передпліччями при русі їх у ліктьових суглобах з опорою. Опорою може бути передня кромка пульта, підлокітники сидіння, уявна точка опори тощо.

При визначенні висоти робочої поверхні стола необхідно урахувати можливість регулювання сидіння крісла по висоті і використання підставки для ніг.

Після змін в організації робочого місця оператора на рисунок необхідно помістити манекен, виготовлений за максимальними розмірами, і перевірити збереження для нього умов зручності робочого місця; маніпулюючи манекенами, домогтися такого положення, щоб робоче місце за столом було містким для оператора з максимальними розмірами тіла, і досяжне для оператора з мінімальними розмірами.

Контури максимального і мінімального манекенів у фізіологічно раціональній робочій позі, кути огляду для кожного з манекенів обвести олівцями різного кольору.

Після вибору параметрів робочого стола треба розмістити на ньому дисплей, у клавіатуру, документи, різні технічні засоби, вказати кути огляду дисплея, документів.

Клавіатуру розташувати в оптимальній зоні моторного поля. Для визначення оптимальної зони моторного поля необхідно виконати таке. На аркуші паперу провести лінію, яка дорівнює найбільшому поперечному розміру (розмір 17, див. табл. 2) мінімального манекена. Від цієї лінії відкласти відстань між передньою поверхнею тіла оператора і краєм робочої поверхні стола, підставки, на якій розташовано дисплей.

Провести другу лінію, на цю лінію спроектувати точки *«М» і «N».* Із отриманих точок «О» і *«К»* (точки опори ліктями), як із центрів, провести дуги радіусом, що дорівнює довжині ліктьово-пальцьової точки Ш (довжина передпліччя і кисті - розмір 6) оператора мінімальних розмірів. Це і буде та відстань, на якій розміщують клавіатуру

4.3. Ергономічна оцінка організації діяльності оператора за дисплеєм

При виконанні роботи в конкретних умовах діяльності оператора за дисплеєм ергономічну оцінку організації

робочого місця необхідно проводити за наступними параметрами:

- висота робочої поверхні стола;
- розміри простору для ніг: висота, ширина, глибина, відстань від поверхні сидіння крісла до нижнього краю робочої поверхні;
- відстань від очей оператора до екрана дисплея;
- висота розташування екрана дисплея на столі або підставці по куту між нормаллю до центра екрана і горизонтальною лінією погляду;
- кут спостереження екрана в горизонтальній площині при роботі за одним дисплеєм; кут розвороту екрана відносно оператора при наявності трьох і більше дисплеїв на робочому місці;
- розташування документів на робочому місці, що визначає кут між екраном алфавітно-цифрового дисплея (**АЦД**) і документом у горизонтальній площині;
- розміщення пульта з клавіатурою на поверхні стола чи підставці;
- розміщення пульта функціонального контролю на робочому місці;
- розміщення пульта зв'язку і телефонних апаратів на робочому місці;
- розміщення пристроїв документування, введення-виведення інформації на перфострічку та інших технічних засобів на робочому місці;
- вага пульта і можливість пересування його на робочому столі, підставці;
- розташування робочого місця щодо напрямку погляду оператора;
- яскравість екрана **АЦД**, перепад яскравості поверхні екрана, документів, клавіатури; рівень освітленості документів;
- контраст екрана **АЦД** (прямий, зворотний);
- кількість знаків, які одночасно з'являються на екрані дисплея; достатність для виконання поставленого перед

оператором завдання; накреслення знаків, можливість помилки при їх сприйнятті;

- розміри алфавітно-цифрових знаків; співвідношення між висотою та шириною знака; висотою і товщиною обведення знака; відстань між знаками; відстань між рядками;
- розрахунок кількості знакомісць на екрані електронно-променевої трубки (**ЕПТ**);
- яскравість кольорової **ЕПТ;** яскравість знаків алфавітно-цифрової інформації; нерівномірність яскравості нуля; кількість відтворених кольорів;
- висота клавіатури відносно поверхні підлоги; кут нахилу клавіатури; розмір квадратних клавіш по діагоналі; зусилля, які необхідні для приведення клавіш у рух; амплітуда руху клавіш; відстань між сусідніми клавішами; поверхня клавіш (блискуча, матова); захищеність поверхні клавіш від стирання; розташування букві цифр на клавіатурі;
- кількість функціональних клавіш; їх достатність для виконання поставленого завдання; відмінність функціональних клавіш від звичайних (колір, форма, положення, відстань); засоби попередження випадкового вмикання клавіш; символічні позначення на клавішах;
- засоби удосконалення світлотехнічних характеристик **АЦД**;
- розширення засобів структурування інформації **АЦД**;
- забезпечення ергономічно обґрунтованого темпу зміни інформації **АЦД**;
- крісло оператора: висота сидіння, можливість регулювання висоти сидіння і спинки й кутів їх нахилу;
- санітарно-гігієнічні умови праці: мікроклімат (температура, вологість, рухливість повітря на робочому місці) та рівень шуму;
- режим праці й відпочинку;
- час безперервної роботи за дисплеєм.

4.Завдання лабораторної роботи.

4.1. Ознайомлення з технікою безпеки роботи пристроїв з відеодисплейним теміналом

4.2. Ознайомитись з ергономічними вимогами до робочого місця оператора відеодисплейного терміналу та спроектувати робоче місце викладача комп`ютерного класу на 12 робочих комп`ютеризованих місць; та робоче місце студента в комп`ютерному класі на 12 робочих місць.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Охарактеризуйте поняття робочого місця оператора за дисплеєм.
2. Що розуміють під моторним полем робочого місця оператора **СЛМ**?
3. Охарактеризуйте зони досяжності моторного поля робочого місця оператора **СЛМ**.
4. Які технічні засоби використовуються в складі робочого місця оператора **ЕОМ** ?
5. В чому полягають загальні ергономічні вимоги до розміщення технічних засобів на робочому місці ?
6. Якими є ергономічні вимоги до розміщення дисплея на столі, підставці (відстань від очей до екрана дисплея, кут спостереження, розвороту тощо) ?
7. Охарактеризуйте ергономічні вимоги до яскравості, контрасту екрана та розмірів алфавітно-цифрової інформації.
8. Як розрахувати кількості знакомісць на екрані **АЦД** ?
9. Охарактеризуйте ергономічні вимоги до кольорових **ЕПТ.**
10. Якими є ергономічні вимоги до розміщення пульта дисплея на робочому місці, клавіатурі та функціональних клавіш ?
11. Охарактеризуйте ергономічні вимоги до світлотехнічних характеристик **АЦД.**
12. В чому полягають ергономічні вимоги до засобів структурування інформації ?
13. Якими є ергономічні вимоги до темпу зміни інформації **АЦД** ?
14. Наведіть загальні ергономічні вимоги до робочого місця оператора за дисплеєм.

ТЕМА-6. ВИВЧЕННЯ ОСНОВ ІМОВІРНІСНОГО АНАЛІЗУ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

1.Мета роботи.

Ознайомлення з основними управління ризиками та методами імовірнісного аналізу безпеки інформарційно-комунікаційних систем.

2.Необхідні матеріали.

1.В.В. Бегун, І.М. Науменко // Безпека життєдіяльності (забезпечення соціальної, техногенної та природної безпеки). -Київ. Видавництво УАННП “Фенікс”.-2004. - 327 с.

2.В.В.Бегун, О.В. Горбунов, И.Н. Каденко и др. // Вероятностный анализ безопасности атомных станций. - Киев. -2000. - 563 с.

3.О.К. Шуаібов, І.Й. Росола Теоретичні основи та логічні моделі безпеки життєдіяльності. Ужгород. 2007. Видавництво УжНУ «Говерла». 307 с.

3.Основні теоретичні відомості.

3.1. Управління ризиками. Методи оцінки ризику.

Оцінка та управління ризиками (**Loss Control Management**) здійснюються в США з 1978 року. Вони охоплюють економічні, фінансові, страхові та інші ризики. В Європейському Союзі оцінка ризику передбачена директивою 1989 року **89/391.EW9**. Систематична ідентифікація небезпек дозволяє виявляти і своєчасно усувати їх. Джерелами небезпек можуть бути технологія, організація праці, поведінка працівників, природні явища та інші чинники. Ризик може бути *припустимий* і *неприпустимий*. У стандарті **OHSAS 18001** термін "*безпека*" визначений як відсутність неприпустимого ризику. Це означає, що працівник повинен знати, які заходи безпеки слід

застосовувати, щоб не перевищувати рівень припустимого ризику. Керівники робіт і працівники повинні вміти ідентифікувати й оцінювати ризики.

Приступаючи до ідентифікації небезпек на робочому місці, необхідно виявити всі небезпеки, які можуть призвести до нещасного випадку, неодмінно передбачити тяжкість наслідків та імовірність одержання травм, захворювання, аварії чи пожежі.

Існує багато методів оцінки професійного ризику на робочих місцях:

—класична методика (Британський стандарт **BS-8800**);

—граф оцінки ризику;

—Risk score;

—Risk assessment code та ін.

Однак варто зауважити, що зовсім недостатньо тільки один раз здійснити оцінку ризику на робочому місці. Необхідно його систематично перевіряти і вживати відповідних корегувальних заходів з метою запобігання відхиленням від норм, правил, інструкцій з охорони праці з метою недопущення неприпустимого ризику. Якщо вчасно не усунути неприпустимий ризик, то травма або хвороба про це нагадає. Необхідно щоденно здійснювати моніторинг ступеня ризику робіт.

Класична методика оцінки професійного ризику здійснюється за формулою: **R=PS** , де **R** — професійний ризик; **P** — імовірність події; **S** — тяжкість наслідків.

Нехай імовірність події буде: **A** — висока; **B** — середня; **C** — низька. Тяжкість наслідків розподілимо таким чином: **I** — аварія, загибель потерпілого; **II** — важка травма; **III** — легка травма. Тоді категорія ризику буде: 5 — дуже високою; 4 — високою; 3 — середньою; 2 — низькою; 1 — дуже низькою, (табл.1). Із табл.1 випливає, що рівень ризику підвищується пропорційно збільшенню ймовірності події і тяжкості наслідків. На підставі цієї таблиці встановлюється категорія ризику, а за необхідності — вживаються запобіжні заходи.

Таблиця 1. Рівень ризику залежно від імовірності події та тяжкості наслідків

Тяжкість	Імовірність події		
	A висока	B середня	C мала
I. Велика	5 дуже високий ризик неприпустимий	4 високий ризик неприпустимий	3 середній ризик припустимий
II. Середня	4 високий ризик неприпустимий	3 середній ризик припустимий	2 низький ризик припустимий
III. Мала	3 середній ризик припустимий	2 низький ризик припустимий	1 дуже низький ризик припустимий

Наприклад, столяр має намір розпиляти дошку на циркулярній пилі зі знятим огородженням. Це може призвести до порізу руки. Тяжкість наслідків — середня (**II**), імовірність події — висока *(**A**)*. За табл.1 визначаємо категорію ризику (4 — високий ризик, неприпустимий). Отже, запланована робота не може бути розпочата до встановлення огородження.

Така методика ідентифікації та оцінки професійного ризику може бути застосована для прийняття рішення про можливість розпочати будь-яку роботу або вжити заходів щодо зниження категорії ризику. Таким способом і здійснюється управління ризиками.

«**Карта оцінки ризику**» може бути додатком до «**Карт умов праці**», які застосовуються для визначення пільг і компенсацій працівникам. «**Карта оцінки ризику**» є механізмом усунення небезпек на робочих місцях.

Оцінка професійного ризику повинна здійснюватися перед пуском обладнання, здачі робочого місця в експлуатацію, а в подальшому — при змінах у конструкції обладнання, організації праці, технологічному процесі, а також у разі аварії чи травми працівника. Працівник повинен бути ознайомлений з результатами ідентифікації й оцінки категорії професійного ризику та з проведеними заходами щодо його зменшення.

Категорія ризику робочого місця визначається за найвищим його значенням по обстежених факторах. Наявність факторів III, IV класів у «**Карті умов праці**» або порушення вимог інструкції з охорони праці підвищує категорію ризику на одиницю. За результатами оцінки ризику розробляються заходи щодо його зниження до припустимого рівня.

Граф оцінки ризику: R = S·E·B·P,

де **R** — ризик; **S** — очікувана шкода; **E** — експозиція небезпеки; **B** — захист від небезпеки; **P** — ймовірність дії небезпеки. Згідно з опублікованими даними (***Boesten I.M.* Bedrijfsongevallen, Samson, Alphen oan de Rijn. — Deurme, 1991.**), параметри оцінки ризику будуть такими.

Очікуваний обсяг шкоди - **S***:*

- **S1** — легке ушкодження, або дискомфорт;
- **S2** — тяжке, або незворотне, ушкодження однієї чи кількох осіб;
- **S3** — загибель однієї особи;
- **S4** — загибель кількох осіб.

Час дії, експозиція небезпеки на працівника - **E***:*

- **E1** — поодинокі, до частого виникнення, небезпеки;
- **E2** — часті, до постійного виникнення, небезпеки.

Захист від небезпек - **B**:

- **B1** — ефективний за виконання вимог безпеки;
- **B2** — не дає ефекту.

Імовірність виникнення небезпеки - **P**:

- **P1** — дуже мала імовірність;
- **P2** — мала імовірність;
- **P3** — відносно велика імовірність;

На рис.1. наведено граф для визначення категорії ризику.

Розглянемо приклад оцінки ризику за методикою **Risk shore:**

$$R = S \cdot E \cdot P,$$

де **R** — ризик; **S** — потенційні наслідки небезпеки; **E** — експозиція небезпеки; **P** — імовірність виникнення небезпеки.

Згідно з опублікованими даними *(***Kinney J. F., Wituth A. D. Practical Risk Analysis for safety management. —■ Naval Weapons centre. China lake, 1976.**)*

Таблиця.2. Risk score — Потенційні втрати

		Розмір витрат	
		людські втрати	матеріальні втрати
100	Велика катастрофа	Багато смертельних випадків	Понад 10 млн дол.
40	Катастрофа	Декілька смертельних випадків	1—10 млн дол.
15	Дуже велика катастрофа	Смертельний випадок	100 тис. — 1 млн дол.
7	Великі	Тяжка травма	10—100 тис. дол.
3	Середні	Тимчасова втрата працездатності	1—10 тис. дол.
1	Малі	Мікротравма	До 1 тис. дол.

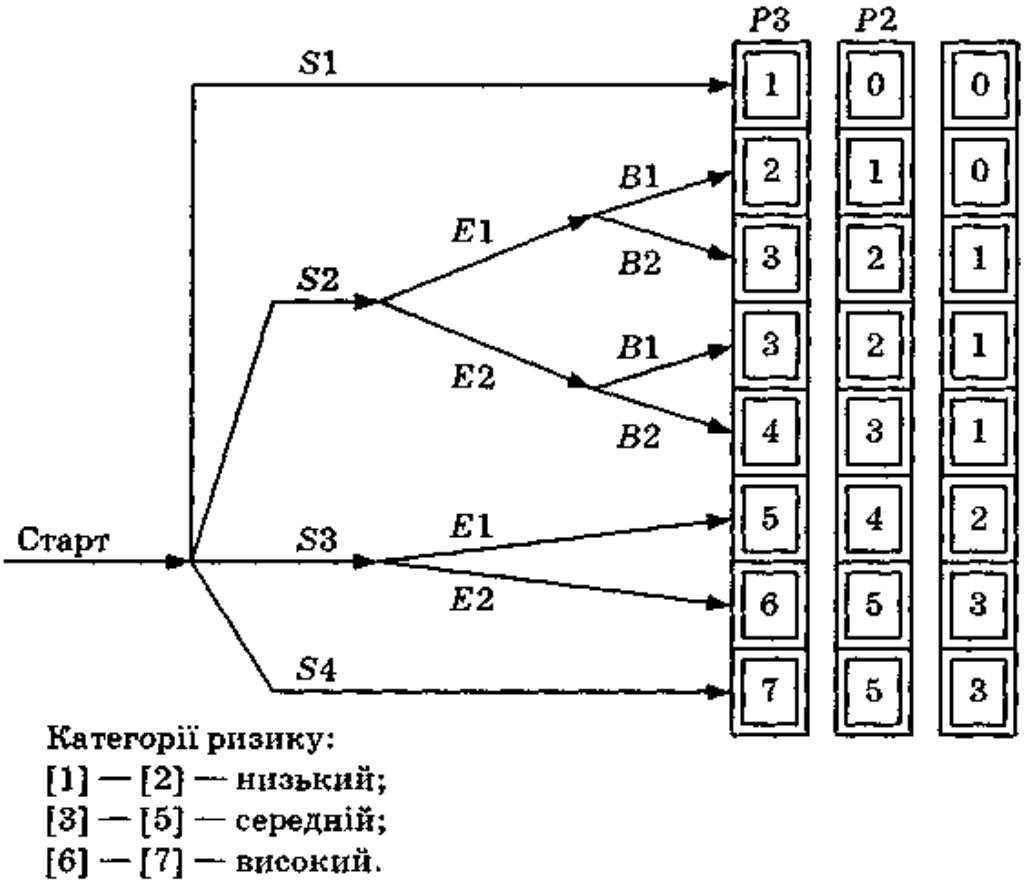


Рис.1. Граф для визначення категорії ризику

Таблиця 3. Дані для методики **Risk score** — експозиція**.**

Вартість	Тривалість
10	Постійна
6	Часта (щоденна)
3	Спорадична (раз на тиждень)
2	Випадкова (раз на місяць)
1	Мінімальна (кілька разів на рік)
0,5	Зникаюча (раз на рік)

Risk score — імовірність

Вартість	Величина	Величина, %
10	Дуже ймовірно	50(1 на 2)
6	Цілком можливо	10(1 на 10)
3	Малоймовірно, але можливо	1 (1 на 100)

1	Тільки спорадично можливо	0,1(1 на 1000)
0,5	Можливо уявити	0,01 (1 на 10 000)
0,2	Практично неможливо	0,001(1 на 100 000)
0,1	Тільки теоретично можливо	0,0001 (1 на 1 000 000)

Risk score — Приклад оцінки ризику

Параметр	Вартість	Кількість балів
Потенційні втрати	Один смертельний випадок	15
Експозиція	Спорадична (раз на тиждень)	3
Ймовірність	Малоймовірно, але можливо	1

$R = 15 \cdot 3 \cdot 1 = 45$

***Risk score* —** Категорії ризику

№ з/п	Категорії ризику	Вартість [Я]	Необхідні заходи
1	*Помірний*	Ж 20	Жодних заходів не потрібно
2	*Низький*	20<і?<70	Треба звернути увагу
3	*Середній*	70<Д<200	Потрібні заходи
4	*Високий*	200 < і? < 400	Необхідні негайні заходи
5	*Дуже високий*	Д<400	Потрібно припинити роботи

Сутність мпетодики **«risk assessment code»** описує вираз*:* **R = S· P**, де **R** — ризик; **S** — потенційні втрати; **P** — імовірність.

Таблиця 4. Основні параметри методики «**risk assessment code»**

	Непр-ипуст-імі	Неба-жані	Малі	Припу стимі
Дуже імовірно	4	4	3	2
Спорадично	4	3	2	1
Малоймовірно	4	2	1	1
Практично неможливо	3	1	1	1

На підставі опублікованих даних ***(*Booth R. T. U. S. Deparrtment of defense. MILSTAN 882B // System Safety Program Requirements. — Marsh 30. — 1984. — p. A-4.)** одержуємо наступні категорії професійного ризику:

1	Ризик малий, жодних заходів не потрібно, але рекомендується проводити моніторинг небезпек
2	Необхідно проводити моніторинг і контроль ризику
3	Необхідно проводити моніторинг і контроль імовірного ризику
4	Ризик повинен бути усунений або гарантовано контрольований

Ця методика дозволяє підприємству, залежно від матеріальних та інших можливостей, встановлювати категорії втрат.

Таблиця 5. Методика визначення втрат (матеріальних, середовища, людських, продукції)

Втрати неприпустимі	— втрати матеріальні (понад 0,3 млн дол.); — значне забруднення середовища; — смерть або тяжка травма працівника; — втрата продукції протягом трьох днів
Втрата небажана	— втрати матеріальні (понад ЗО тис. дол.); — забруднення середовища; — втрата працездатності (понад ЗО днів); — простій (понад 1 год.)
Мала втрата	— втрати матеріальні (від 300 до ЗО тис. дол.); — підвищена емісія забруднень; — втрата працездатності (від 3 до ЗО днів); — простій (до 1 год.)
Втрата неприпустима	— втрати матеріальні (до 300 тис. дол.); — забруднення середовища; — втрата працездатності до 2 днів; — дрібні неполадки

3.2. Опис методу дерев відмов.

Аналіз дерев відмов систем є найбільш загальним методом, що використовується для представлення логіки відмов технічних систем, зокрема, атомної станції. Він являє собою дедуктивний аналіз відмов, який можна описати аналітично. Метод дозволяє визначити небажаний стан системи і потім аналізувати систему з урахуванням навколишніх умов і умов експлуатації для з'ясування всіх можливих шляхів, за якими може реалізуватися небажана подія.

Дерево відмов являє собою графічну модель різних паралельних і послідовних сполучень відмов, що приводять до реалізації заздалегідь **визначеної** небажаної події. Відмови — це базисні події, що пов'язані з виходом з ладу елементів системи, помилками персоналу, неготовністю устаткування внаслідок технічного обслуговування, іспитів чи інших обставин, що можуть тягти за собою небажану подію.

Таким чином, дерево відмов відображає логічні взаємозв'язки базисних подій, які ведуть до небажаної події, що уявляє собою "**верхню подію**" дерева відмов. Схеми дерев відмов точно визначають логічні комбінації базисних подій, що приводять до верхньої події.

3.3. Розробка дерева відмов технічних систем

Дерева відмов (**ДВ**) являють собою математичні імовірнісні моделі систем, що враховують можливі відмови всіх елементів, що складають систему, їхній взаємозв'язок і взаємозалежність та дозволяють розрахувати імовірність відмови системи на основі відомих характеристик надійності її елементів.

Дерева відмов складаються з базисних подій з'єднаних логічними елементами. Отже, **дерева відмов** — логічні уявлення імовірних відмов систем, що можуть відбуватися і приводити до небажаної події.

Мета використання дерев відмов:

- виявлення шляхів, що приводять до відмови системи;
- вивчення моделі системи шляхом:
- вивчення взаємозалежності між відмовами елементів;
- визначення імовірності відмови системи;
- одержання інформації про "**вразливі місця**" системи, що моделюють.

Умови розробки дерев відмов:

- використання дедуктивного аналізу;
- чітке визначення небажаної події;
- облік взаємозв'язку між подіями;
- використання параметрів неготовності окремих компонентів;
- деталізація вхідної інформації повинна мати відповідний рівень.

Процес розробки дерева відмов схематично зображений на рис.2.

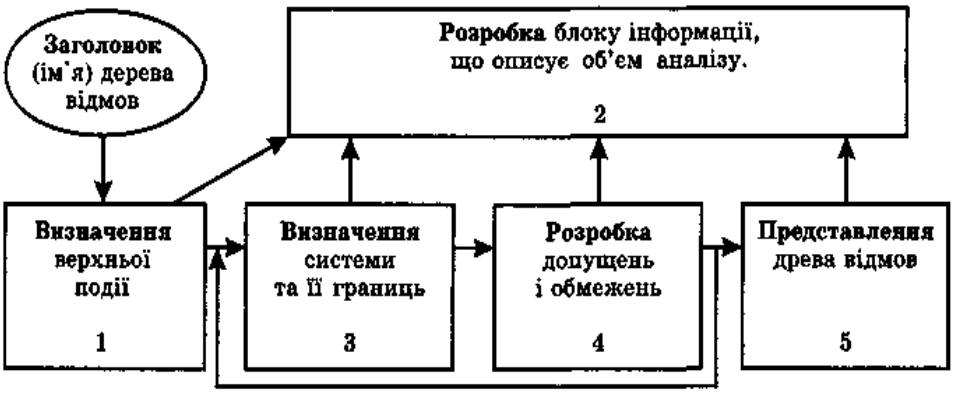


Рис.2. Процес розробки дерева відмов.

Побудову **ДВ** умовно можна розбити на **5** етапів.

1. **Визначення верхньої події.** Верхня подія **ДВ**:

- це небажана подія;
- вона повинна бути конкретною, якщо вона дуже загального характеру, то аналіз буде складний;
- якщо ж вона занадто конкретна, то може загубитися інформація, корисна для аналізу;
- необхідно чітко задавати робочий стан компонентів, що входять у систему.

2. **Розробка блоку інформації, що описує обсяг аналізу**, включає:

- визначення меж системи і визначення даних для аналізу;
- експлуатаційну і проектну інформацію, дані з регламенту;
- облік регламентів ремонту і технічного обслуговування.

3. **Визначення системи та її границь:**

- може відрізнятися від розуміння експлуатації;
- якщо кілька систем виконують одну функцію безпеки то варто представляти її як одну систему, тобто система представляється як набір елементів;
- необхідно чітко визначити границі системи.

4. **Допущення й обмеження, що приймаються** (оскільки немає повної інформації про всі явища):

- основа для припущень повинна бути конкретною і спиратися на детерміністичний аналіз;
- обмеження допомагають визначити обсяг аналізу.

5. **Представлення дерева відмов** — кінцевий етап побудови:

- крок за кроком визначати недоліки систем (декларувати);
- позначення повинні бути зроблені зрозуміло (стандартно);
- при визначенні набору відмов, окремі відмови повинні відповідати ступеню подробиці, прийнятому раніше.

Побудова дерева відмов — це ітераційний процес. Розуміється це в тому значенні, що для складних систем багато відмов можуть розглядатися як у моделях ДВ, так і в інших моделях і для з'ясування цієї обставини необхідна розробка різних варіантів і їх спільний аналіз. Іноді функції системи аналізуються в деревах подій краще, ніж у деревах відмов, тобто можливі переходи доти, поки не буде повної відповідності.

3.4. Основні положення і правила побудови дерев відмов. Приклад.

Вище розглянуті основні принципи й етапи побудови дерев відмов. У цьому пункті розглянемо їх більш докладно і конкретно.

Основні **правила**:

•При побудові **ДВ** використовується концепція миттєвої відмови, тобто кожна подія представляється такою, що відбувається в даний момент.

•Спочатку звертаємо увагу на необхідні і достатні причини виникнення верхньої події, потім причину цієї причини і так далі послідовно по кроках (всіх причинах).

Побудову **ДВ** розглянемо на прикладі каналу подачі води, що складається з трубопроводів, насоса А, засувок В і С паралельних трубопроводів і засувки D, що перекриває загальну ділянку (рис.3).

Приклад побудови **ДВ** каналу подачі води.

Верхня подія — небажана подія: "Відмова проходження потоку через засувку "D" протягом 24 годин". Обмеження "протягом 24 годин" у даному випадку має значення при визначенні імовірностей базисних подій — відмова елементів схеми.

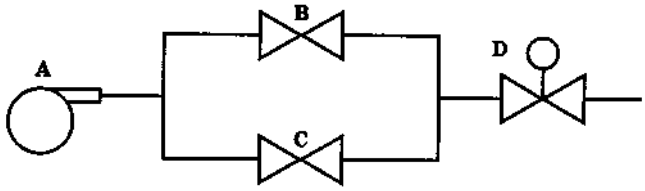


Рис.3. Канал подачі води.

Дотримуючись правил попереднього пункту визначимо можливі причини (базисні події), починаючи з верхньої події:

D1 — відмова засувки "D" відкритися на вимогу, чи

D2 — клапан "D" не зміг залишатися відкритим протягом 24 годин, чи

D3 — не було вхідного потоку — не подія, а причина, тому повинна бути проаналізована ця можливість, тобто визначені необхідні і достатні умови:

B1 — немає потоку з-за засувки B, і

C1 — немає потоку з-за засувки C.

Розглянемо можливі варіанти для обох умов:

BИ — "B" не відкривається на вимогу;

B12 — "B" не зміг залишатися відкритим протягом 24 годин;

B13 — немає вхідного потоку на засувку "B".

Те ж саме для "C":

C11 — "C" не відкривається на вимогу;

C12 — "C" не зміг залишатися відкритим протягом 24 годин;

C13 — немає вхідного потоку на засувку "C".

Продовжуючи процес далі, спускаємося нижче і нижче, одержуємо причини відсутності потоку на засувки "B" і "C":

A1 — насос не запустився на вимогу;

A2 — не зміг працювати протягом 24 годин;

А3 — не було потоку в насос (нерозвинений елемент).

Якщо дуже надійний резервуар, то варто утриматися від розбивки А3 на дрібні відмови.

Повинні бути однаково позначені основні (базисні) події, незалежно від їхнього місця в **ДВ**, якщо вони ті самі, тобто події: А1, А2, А3 для В13 і С13, хоча це і різні гілки **ДВ**.

Дерево відмов "Відмова проходження потоку через засувку "D", побудоване без використання коду "IRRAS" зображене на рис.4.

Приведемо також інші аспекти, які необхідно враховувати при побудові **ДВ** в більш складних задачах:

a). На початку процедури побудови дерев відмов повинні бути погоджені: границі систем, логічні символи, індексація (кодування) подій, а також облік і представлення помилок персоналу і відмов по загальних причинах.

b). Усі допущення, зроблені в процесі побудови дерев відмов, повинні бути відбиті в звітній документації поряд із джерелами використовуваної проектної інформації. Таким шляхом буде забезпечена погодженість дій протягом всього аналізу, а також можливість простежити хід досліджень.

c). Якщо системи не моделюються в деталях і використовуються дані по надійності системного рівня, то події відмов, що є загальними і для інших систем, повинні бути виділені і розглянуті явно.

d). Настійно рекомендується ще до початку аналізу встановлювати ясні і точні визначення границь систем. У ході аналізу необхідно дотримувати встановлених границь, а їхні визначення повинні міститися в підсумковій документації по моделюванню систем.

e). Важливо, щоб застосовувалася стандартизована форма для кодування базисних подій у **ДВ**. Обрана схема повинна бути сумісна з обраним комп'ютерним кодом для аналізу систем і чітко ідентифікувати базисні події з погляду:

—виду відмов устаткування

—визначення виду і типу конкретного устаткування

—приналежності устаткування до конкретної системи

—станційного ідентифікатора устаткування.

f). Дерева відмов повинні відображати всі можливі види відмов, що можуть спричинити неготовність системи. Повинні враховуватися складові, причетні до виводу устаткування з роботи для іспитів і технічного обслуговування. У необхідних випадках потрібно враховувати помилки персоналу, пов'язані з помилковими діями по приведенню устаткування в робочий стан після іспитів і технічного обслуговування, а також з помилковими діями в процесі аварії. Можливі дії персоналу по відновленню працездатності устаткування часто мають специфіку для кожної аварійної послідовності і видів відмов елементів. Ці особливості ефективніше всього враховувати так, як це описано в процедурі виконання задачі кількісного аналізу аварійних послідовностей.

g). У деревах відмов повинні знайти відображення наступні аспекти залежних відмов:

- взаємозалежності вихідних подій і реакцій систем;
- відмови загальних підтримуючих систем, що роблять вплив більш ніж на одну фронтальну систему чи елемент через функціональні залежності;
- помилки персоналу, пов'язані з загальними операціями іспитів і технічного обслуговування;
- загальні елементи фронтальних систем.

При виконанні моделювання треба визначити й описати усі функціональні і системні дерева відмов, які охоплені в аварійних послідовностях. При побудові системних дерев відмов мають бути враховані всі системи, що **забезпечують** роботу системи, які необхідні для виконання функцій безпеки, покладених на систему, тобто системи вентиляції, електропостачання, системи промконтурів і т. інш.

Усі системи у всіх конфігураціях, що ввійшли в модель, мають бути представлені й описані до початку процедури побудови **ДВ**. Метою цієї роботи є визначення здатності виконувати покладені на систему функції безпеки в залежності від стану елементів системи, їхніх видів відмов з урахуванням можливості відновлення в режимі чекання і при

аварії, і визначення на рівні елементів системи міжсистемних зв'язків.

В усіх випадках, де у імовірнісній моделі передбачене втручання персоналу, треба представити й описати дерева відмов для персоналу і всі дії/операції, на підставі яких вони побудовані. Ці події, що пов'язані з відновленням функцій оператором, як і відмови із загальної причини, повинні бути додані в дерева відмов на заключному етапі, в остаточному підсумку.

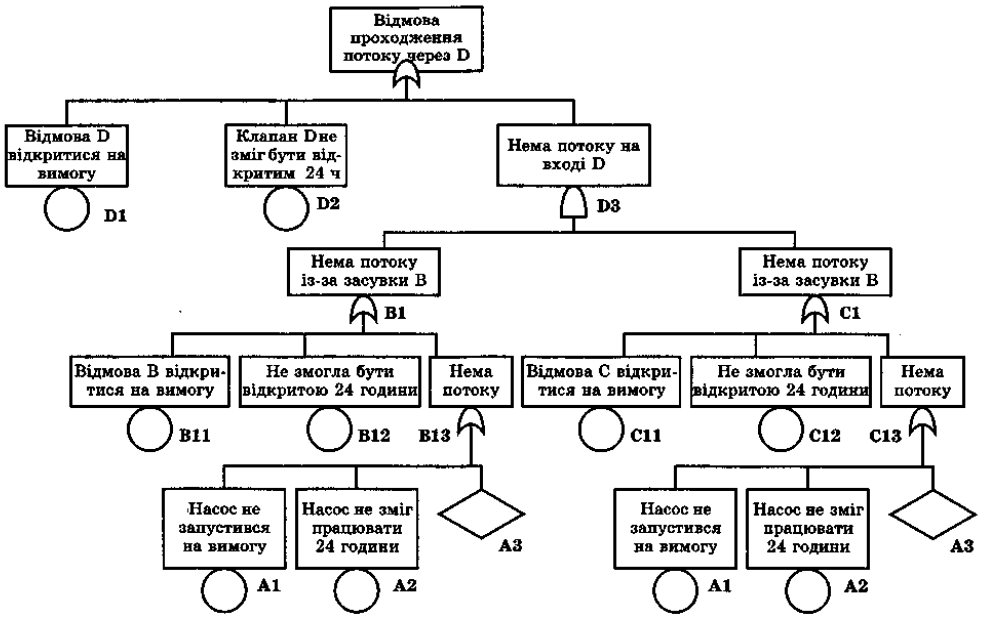


Рис 7.14 ДВ "Відмова проходження потоку через засувку "D"

Рис.4. Відмова проходження потоку через засувку « D».

Розглянемо наступні види відмов устаткування:

• насоси (Pump), дизель-генератори — ДГ (**DG**):

—відмова запуску (failure to start — **FS)**. До даного типу відмов відносяться також вихід устаткування з ладу протягом невеликого часу після запуску (30 хвилин) — мимовільне відключення, підвищені навантаження на відповідальні вузли, підвищені вібрації, температури і т. інш.

—відмова на виконання функцій у заданий час роботи (24 години) (failure to run — **FR**)

• арматура (засувки, регулятори — Motor operated valve (MOV), зворотні клапани — Check valve (**CV**), запобіжні клапани — Reliefvalve (**RV**):

—відмова на відкриття (failure to open — **FC**) — відмова в результаті якої арматура не відкривається, чи відкривається не цілком (не повний прохідний перетин);

—відмова на закриття (failure to close — **FC**) — відмова, в результаті якої арматура не закривається при надходженні вимоги на її закриття, чи закривається не цілком (не повний прохідний перетин);

• бак, ємність, теплообмінник (Tank, Heat exchander):

—течія (leakage — **LK**) таких розмірів, що виконання функції безпеки стає неможливим;

—зниження параметрів середовища (parameters change —**PC**), у результаті чого параметри виявилися нижче необхідних для виконання функцій безпеки.

3.5. Умовні позначки елементів у деревах відмов, які застосовувані в IRRAS.

Позначення базисних подій в коді **IRRAS** визначає і розрізняє, у залежності від вихідних даних кілька типів базисних подій, позначення яких приведені на рис.5.

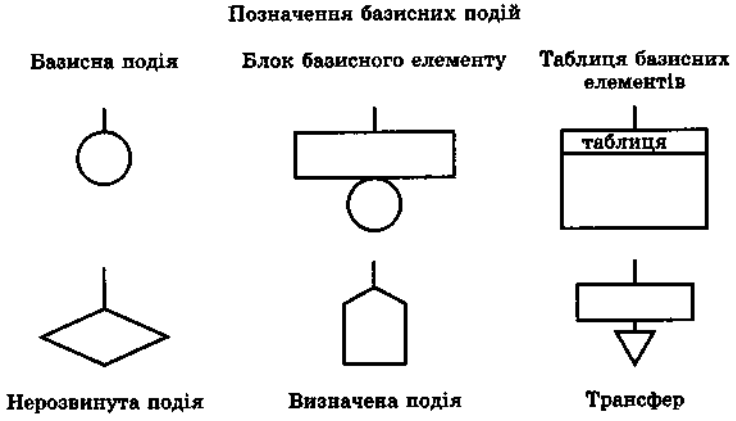
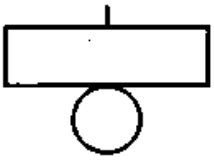


Рис.5. Позначення базисних подій

Коротко розглянемо опис позначень базисних подій.

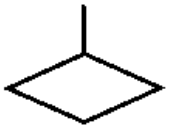
1). Базисний елемент — (**Basic Event_A**) — базисна подія являє ушкодження чи дефект — це відмова устаткування, людська помилка чи несприятлива умова. Коло означає, що подія відмови не вимагає подальшої розробки.



2) Прямокутний базисний елемент — додатковий символ для базисної події — подія, яка містить у прямокутному елементі короткий опис базисної події.

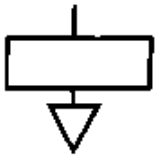
3)

3) Таблиця основних базисних елементів — дозволяє включити від 3 до 8 базисних подій, що будуть уведені компактно в схему **ДВ**. Логіка, що використана в таблиці, диктується логічним елементом (**gate**), що з'єднує елементи в дереві відмов.



4) Неописана (нерозвинена) подія — позначає базисну подію, що є фактично більш складною подією, що не була далі розвинута логікою дерева відмов. **IRRAS** обробляє цю подію інакше, ніж базисну подію.

5) Елемент типу "дім" (**House**) — визначена подія, використовується, щоб позначити відмову, яка гарантовано завжди відбудеться чи ніколи не відбудеться. Тип обчислення, приписуваний базисній події, установлює є чи ні подія подією типу "**дім**". Будь-яка базисна подія в **IRRAS** може бути визначена подією типу "**дім**".



6) Трансфер — неописане продовження яке вказує, що подія складена досить комплексно, щоб мати власну логіку дерева відмов, розвиту в іншому місці (на іншій сторінці). Однак, подія оброблялася як базисна подія в присутнім дереві відмов.

У коді **IRRAS** можуть бути використані фактично всі логічні операнди булевої алгебри. Значення операндів відповідають раніше визначеним. **IRRAS** визначає і розрізняє їх, відповідно до рис.6. Код **IRRAS** дозволяє визначити й описати нові логічні функції й елементи з подальшим їх використанням як стандартних.

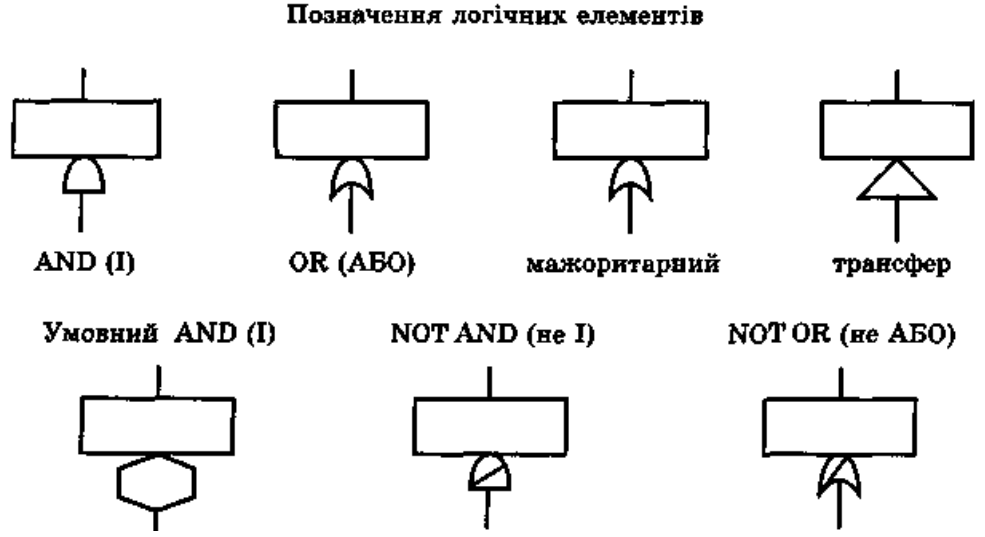


Рис.6. Позначення логічних елементів

Опис основних логічних елементів

1. **AND** (І) — усі входи (базисні події) до кон'юнктуру повинні відбутися, щоб подія відбулася.
2. **OR** (АБО) — один вхід до АБО елементу приведе до відмови.
3. Мажоритарний логічний елемент — **N/M** (**Gate_This**) визначає що, N з M вхідних подій повинне відбутися для відмови. Для елементу 2/3, будь-яка комбінація 2 із 3 вхідних подій має відбутися.
4. Елемент переходу — трансфер — використовуються, щоб зв'язати логічні структури разом без того, щоб представити будь-яку нову логіку власною. Елемент трансфер указує, що логіка продовжена на новій сторінці (чи на тій же самій сторінці). Назва (ім'я) елементу переходу повинно бути таким же як елементу, де логіка продовжується, і при переході до іншої сторінки(окремий файл дерева відмов), повинне бути верхнім елементом на сторінці. Верхня вхідна назва (ім'я) дерева відмов повинна завжди бути ім'ям файлу дерева відмов.
5. Умовний елемент **AND** (І) — використовується, якщо одиночна подія відбувається при визначеній умові. Таким чином, може використовуватися як елемент заборони — спеціальний тип кон'юнктура. Подія з умовним **AND** обробляється просто як базисна подія з імовірністю або як подія типу "дім".

3.6. Моделювання функцій безпеки і систем, що їх виконують

Моделювання функцій безпеки (**ФБ**) і систем, що їх виконують, являє собою моделювання дерев відмов для систем, що виконують необхідні **ФБ** стосовно кожної вихідної події аварії з обраних у межах розглянутих експлуатаційних станів. Метою даної роботи є визначення для кожної системи безлічі можливих відмов і їхніх наслідків, комплексна оцінка імовірностей невиконання заданих **ФБ** і визначення сумарної частоти виникнення вихідних подій

аварій унаслідок відмов елементів системи. Невід'ємною частиною моделювання є опис і якісний аналіз системи, що включає в себе аналіз видів відмов устаткування і їхній вплив на працездатність розглянутої системи — аналіз надійності системи. У рамках аналізу надійності технологічних систем безпеки необхідно врахувати відмови елементів управляючих і обчислюючих систем, безпосередньо пов'язаних з розглянутою системою. Кожна система може мати одне чи декілька **ДВ**, у залежності від кількості виконуваних нею **ФБ** і необхідних при цьому критеріїв успіху. Наслідки відмов допоміжних систем, підсистем і елементів повинні відповідати конструкторській документації і досвіду експлуатації.

Аналіз надійності системи стосовно виконуваних нею функцій безпеки припускає проведення якісного і кількісного аналізів.

Якісний аналіз надійності системи проводиться з метою розробки детальних імовірнісних моделей для наступного кількісного аналізу і містить наступні етапи.

1. Виділення характерних рис структури системи і режимів її функціонування для виділених **ФБ**.
2. Визначення умов і критеріїв виконання **ФБ** з урахуванням тимчасових характеристик.
3. Визначення границь системи і переліку вхідних у неї елементів, що враховуються в аналізі надійності.
4. Аналіз дій персоналу.
5. Аналіз регламенту технічного обслуговування (контролю і ремонту елементів, визначених у п. 3) з урахуванням помилкових дій персоналу.
6. Детальна класифікація видів і наслідків відмов елементів.

Результати розрахунку представляються у вигляді таблиць із значеннями імовірностей невиконання системою заданих **ФБ** з урахуванням незалежних відмов устаткування, відмов устаткування з загальної причини і помилкових дій персоналу.

4.Завдання лабораторної роботи.

4.1. Ознайомлення з методикою побудови матриць ризику та методом дерева відмов, які можуть використовуватись при аналізі ризиків в інформарційно-комунікаційних системах.

4.2. Побудувати дерево відмов, для одного з наступних варіантів негативних (верхніх в дереві) подій:

А). витік конфіденційної інформації чрез канал несанкціонованого доступу в систему ззовні;

Б). втрата диску з інформацією «для службового використання»;

В). спотворення інформації в файлі з конфіденційною інформацією, що належить державі;

Г). витік таємної інформації через канал заземлення;

Д). витік інформації для службового користування через несанкціоноване включення в зовнішню мережу.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Охарактеризуйте види ризиків та методи їх оцінки.
2. В чому полягає сутність класичної методики оцінки ризиків ?
3. Як оцінити ризики за допомогою «графів оцінки ризиків» ?
4. Охарактеризуйте методики «**Risk score**», «**Risk assesimtnt code**» та їх типові характеристики.
5. В чому полягає метод відмов, як метод аналізу ризиків ?
6. Чим зумовлені відмови у роботі технічних систем ?
7. Якими є мета використання і умови розробки дерев відмов ?
8. Охарактеризуйте основні етапи побудови дерев відмов.
9. Якими є основні правила побудови дерев відмов ?
10. Охарактеризуйте особливості побудови дерев відмов складних систем.
11. Наведіть основні позначення подій в коді **IRRAS.**
12. Охарактеризуйте базові логічні елементи коду **IRRAS**.
13. В чому полягає основний зміст моделювання функцій безпеки складних систем ?

ТЕМА-7. ВИВЧЕННЯ ОСНОВНИХ ЕЛЕМЕНТІВ ЗАХИСНОГО ЕКРАНУВАННЯ ФІЗИЧНОГО СЕРЕДОВИЩА, В ЯКОМУ РОЗТАШОВАНА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА

1. Мета роботи.

Ознайомлення з основами технічного захисту середовища розташування інформаційно-комунікаційної системи та передавання з неї інформації, зокрема, екрануванням. Усвідомлення значення екранування інформаційно-комунікаційних систем, засвоєння основ розрахунку та ознайомлення з типовими конструкціями систем екранування.

2. Необхідні матеріали.

1. А. Шваб Измерения на высоком напряжении: Измерительные приборы и способы измерения. Перевод с немецкого. –М.: Энергоатомиздат. 1983. С. 23-32 (264с.).
2. О.К. Шуаібов Практикум з охорони праці. Навчальний посібник. –У.: Видавництво ДВНЗ «УжНУ» «Говерла». 2008. – 279 с.

Основні теоретичні відомості.

3.1. Загальні відомості про екранування приміщень

Для повного усунення наведень від технічних засобів передавання інформації у приміщеннях, лінії яких виходять за межі контрольованої зони, потрібно не тільки різко зменшити їх величину у провідниках, що надходять від джерела, а й обмежити сферу дії електромагнітного поля, яке створюється системою його внутрішніх електропроводок. Ця задача розв'язується шляхом екранування.

Теоретично, з погляду вартості матеріалу і простоти виготовлення, переваги віддаються екранам із листової сталі. Проте застосування металевої сітки значно спрощує питання

вентиляції та освітлення. Аби розв'язати питання про матеріал екранів, необхідно знати, в скільки разів потрібно послабити рівні випромінювання технічних засобів передавання інформації. Найчастіше це - в 10-30 разів. Таку ефективність забезпечує екран, виготовлений із одинарної мідної сітки з комірками 2,5 мм або з тонколистової оцинкованої сталі товщиною 0,51 мм і більше.

Металеві листи (або полотнища сітки) мають бути між собою електрично з'єднані по всьому периметру, що забезпечується електрозварюванням або пайкою. Двері приміщень також слід екранувати із забезпеченням надійного електроконтакту з дверною рамою по всьому периметру не рідше, ніж через 10-15 мм. Для цього застосовують пружинну гребінку з фосфористої бронзи, зміцнюючи її по всьому внутрішньому периметру дверної рами. За наявності в приміщенні вікон їх затягують одним або двома прошарками мідної сітки з коміркою не більше 2х2 мм, причому, відстань між прошарками сітки повинна бути не меншою за 50 мм. Обидва прошарки сітки повинні мати гарний електричний контакт зі стінами приміщення, що забезпечується тією ж гребінкою з фосфористої бронзи або пайкою (якщо сітка незнімна).

Розміри екранованого приміщення вибираються, виходячи з його призначення, наявності вільної площі і вартості робіт. Як правило, достатньо мати екрановане приміщення площею 6-8 $м^2$ при його висоті 2,5-3 метра.

Зазначимо, що всі технічні засоби передавання інформації випромінюють побічні електромагнітні випромінювання і наведення, які можуть бути перехоплені і розшифровані за допомогою спеціальної апаратури.

Перехоплення побічних електромагнітних випромінювань і наведень може бути відвернено відповідним екрануванням всього устаткування технічних засобів передавання інформації і мережевих кабелів для того, аби інтенсивність їх випромінювання різко зменшувалась. Крім того, можна використовувати спеціальні генератори «білого шуму» для захисту від побічних електромагнітних

випромінювань і наведень, наприклад «**ГБШ-1**», «**САЛЮТ**», «**ЗАВІСА**», «**ГРІМ**» тощо.

Виникнення наведень у мережах живлення технічних засобів передавання інформації найчастіше пов'язано з тим, що вони ввімкнені до загальних ліній живлення. Тому мережеві фільтри виконують дві функції в ланцюгах живлення технічних засобів передавання інформації:

- захист апаратури від зовнішніх імпульсних перешкод;
- захист від наведень, створюваних самою апаратурою.

При цьому, однофазна система розподілу електроенергії повинна здійснюватися трансформатором із заземленою середньою точкою, трифазна - високовольтним знижувальним трансформатором.

При виборі електричних фільтрів слід враховувати:

- номінальні значення струмів і напруг у ланцюгах живлення, а також допустимі значення падіння напруги на фільтрі при максимальному навантаженні;
- допустимі значення реактивної складової струму на основній частоті напруги живлення;
- необхідне згасання сигналу після проходження фільтру;
- механічні характеристики фільтра (розмір, масу, тип корпуса, спосіб установки);
- міру екранування фільтра від сторонніх полів.

Фільтри в ланцюгах живлення можуть мати найрізноманітніші конструкції, їх маса коливається в межах від 0,5 кг до 90 кг, а об'єм від 0,8 м^3 до 1,6 м^3.

Конструкції фільтрів повинні забезпечувати істотне зниження імовірності виникнення всередині корпусу побічного зв'язку між входом і виходом системи через магнітні, електричні або електромагнітні поля.

3.2. Електромагнітна сумісність та система екранування

При першому вмиканні вимірювального пристрою з реєстрації імпульсів напруги чи сструму. що складається з дільника або шунта, з`єднувльного кабеля і осцилографа, звично одержують осцилограму, наведену на рис.1. Вона, як

правило, не відповідає дійсній зміні в часі напруги або струму, що досліджується. На сигнал, що вимірюється U(t), накладається напруга завад, яка різними шляхами проникає до пластин осцилографа. Це ілюструє необхідність екранування, в даному випадку, осцилографа. В системах захисту інформайійно-комунікаційних систем екрануванню підлягає комп`ютерна система.

Причинами появи завад, які підлягають екрануванню, служить генерація електричних потенціалів і електромагнітних полів, зв`язаних з швидкозмінними напругами і струмами, зокрема із заряджанням і розряджанням паразитних ємностей при вимірюванні паразитних електромагнітних полів. Витік електромагнітного випромінювання з **ІКС** за своєю природою має тіж причини, що і поява спотвореного зображення на екрані осцилографа. Причинами цього явища є наступні чинники.

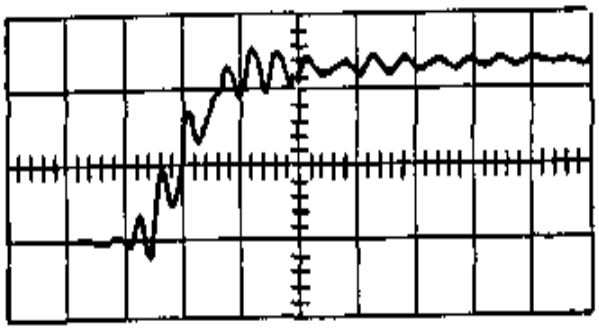


Рис.1. Осциллограма аперіодичного імпульсу струму з завадами в формі накладання високочастотних коливань.

1. Електромагнітне поле проникає через неповністю екранований корпус осцилографа і приводить до прямих спотворень амплітуди сигналу. Це явище може бути виключено (або мінімізовано) шляхом поміщення осцилографа в екрановану кабінку (рис.2). Часто достатньо використати металевий ящик, відкритий з однієї сторони. Вплив електромагнітного поля завад послаблюється при збільшенні віддалі між осцилографом і контуром з струмом.

Повністю екрановані вимірювальні кабінки послаблюють завади на 80-100 Дб при частотах f < 30 ГГц. Це відповідає коефіцієнтам екранування 10^{-4}-10^{-5}.

2. Квазістаціонарні магнітні і електричні поля проникають в неповністю екрановані вимірювальні кола. Електричні поля, що проникають через отвори в плетеній оболонці кабелю, безпосередньо індукують на жилі кабеля напругу завади. Але ці завади в більшості випадків є знехтувано малими порівняно з завадами, які генеруються протіканням струмів по оболонці кабеля.

3. Осцилограф сприймає завади (f < 30 ГГц) по провідникам живлення, які доцільно зменшувати шляхом живлення осцилографа через вводи-фільтри. Такі фільтри складаються з двох ємнісних елементів і одного індуктивного, ввімкнених за П – подібною схемою.

На рис.3. приведені схеми заміщення такого вводу-фільтра з широкою смугою запирання і залежність затухання від частоти.

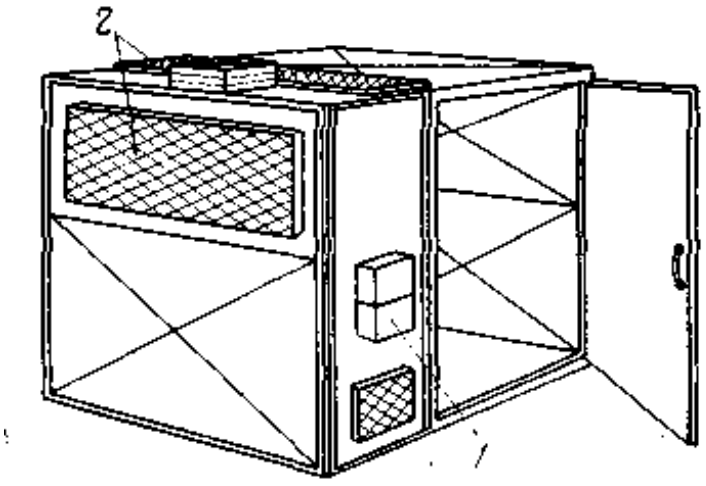


Рис.2. Повністю екранована рухома вимірювальна кабінка: 1 – блок мережевого живлення з пристроями подавлення завад, які поширюються через мережу живлення; 2 – вікна-решітки для освітлення і вентиляції.

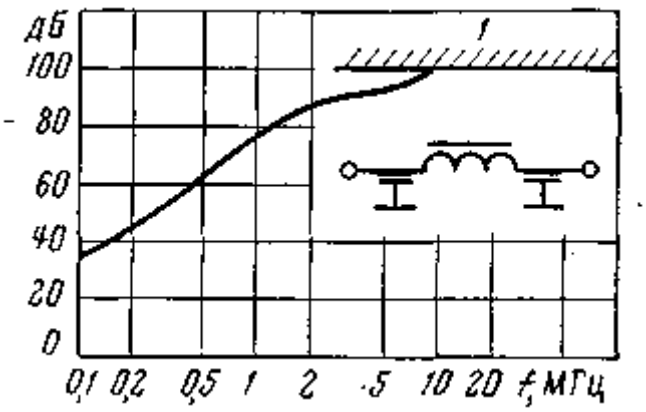


Рис.3. Характеристики затухання широкосмугового фільтру-вводу фірми Siemens (тип B 85321 ABO 1), яка була виміряна разом з кабелем із Z_C = 60 Ом: 1 — границя виміру.

Для хорошої фільтрації в широкому діапазоні частот такий фільтр вбудовується в стінки екрану, що є корпусом осцилографа і одночасно проводиться його екранування. Інколи достатньо провід мережевого живлення намотати на феритовий сердечник чи помістити в гибкий металорукав, що має добрий контакт з корпусом екрану і з корпусом осцилографа.

4. Струми по оболонці кабеля і корпусу викликають появу різних потенціалів на провідниках заземлення. Спад напруги в цьому випадку генерується за рахунок електромагнітних зв`язків з вимірювальними провідниками, що і спричинює завади. Коли по оболонці кабеля чи екрану проходит струм, зумовлений зовнішнім джерелом напруги, то він викликає спад напруги і на їх внутрішніх поверхнях. Він може бути вже помітною завадою в системі провідників, які заключені всередину оболонки кабеля. Опір на одиницю довжини (1), зумовлений електромагнітним зв`язком може бути визначений у відповідності з даними рис.4.

$$z_{св}(t) = u_п(t)/i_ш(t)\, l, \quad , \qquad \textbf{(1)}$$

Тут допущено, що довжина кабеля «l» менша чверті довжини хвилі сигналу, що вимірюється. Чим менший опір зв`язку коаксіального кабеля, тим кращою є його екрануюча дія і тим менша напруга завади. Інколи для зменшення опору зв`язку використовують кабелі з подвійною (потрійною) оболонками або кабелі з суцільною металевою оболонкою, що добре проварена на швах.

На рис.5. приведені залежності опору зв`язку від частоти для такого кабеля (1) і звичайного кабеля з плетеною оболонкою (2).

Розглянемо основні причини, які викликають струми в оболонках кабелів та способи їх мінімізації.

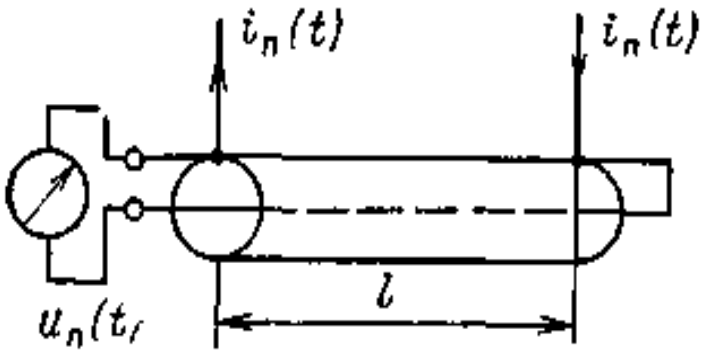


Рис.4. До визначення опору зв`язку **Zзв** (t) коаксіального кабеля.

3.3. Індукована і наведена електрорушійна сила, що пов`язана з швидкозмінними процесами. Зміщення потеціалу в розрядному колі

Для забезпечення електробезпеки корпуси приладів звично з`єднують з нульовим провідником багатофазної мережі живлення чи під`єднують до контуру заземлення. По провідникам заземлення проходять струми навантаження приєднаних до мережі користувачів. а в нульовому проводі

проходить частина струму живлення даного приладу. Із-за електричного сполучення корпусу приладу з заземленням по

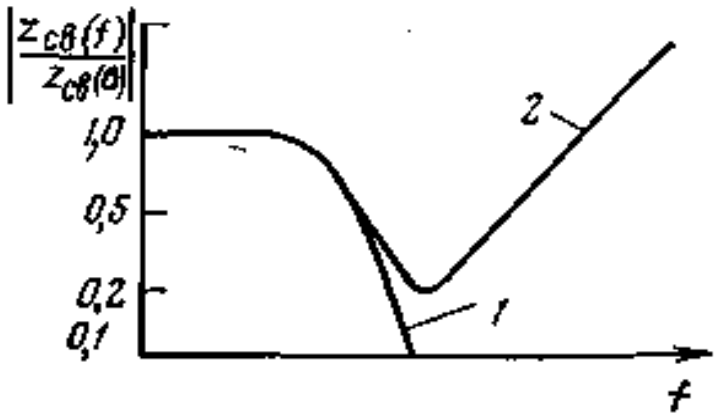


Рис.5. Опір $\mathbf{Z_{зв}}$ гибкого кабеля з гофрованою металевою оболонкою (1) та звичайного кабеля (2).

з`єднувальному провіднику може проходити деякий струм мережевої частоти. Він спричинює спад напруги вздовж проводу заземлення і між зажимами заземлення і заземленими частинами виводів чи розйомів на вході. Внаслідок цього на корпусі осцилографу може появитись помітна напруга. Якщо електричні прилади, що знаходяться поряд, живляться від різних розеток, то оболонки вимірювальних кабелів утворюють заземлені контури. В цих петлях проходять вирівнювальні струми, які генерують завади, що мають частоту мережі живлення. Для мінімізації цього явища необхідно розірвати петлі заземлення і залишити лише один прилад з проводом заземлення.

Правила техніки безпеки в цьому випадку не порушаться, оскільки між заземленим приладом та іншими приладами, безпосередньо не зв`язаними з контуром заземлення, існує електричний зв`язок по оболонкам вимірювальних кабелів.

Квазістаціонарні електромагнітні поля наводять на оболонці кабеля та індукують в контурі «оболонка кабелю-

земля» ЕРС, які викликають проходження струмів в оболонках кабеля і корпусах приладів (рис.6.).

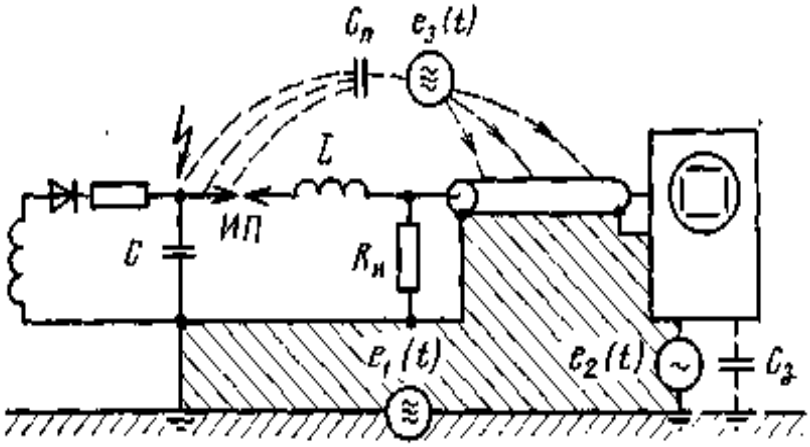


Рис.6. Схематичне представлення виникнення струмів в оболонці кабеля за рахунок індукованої і наведеної ЕРС і різниці потенціалів між заземленими точками вимірювальної петлі: ИП – іскровий проміжок, С – ємність генератора, $R_И$ – шунт, L –індуктивність генератора, **$e_1(t)$** — індукована ЕРС контурі заземлення; **$e_2(t)$** — індукована ЕРС в захисному проводі заземлення, **$e_3(t)$** — наведена ЕРС.

Дія обох полів послаблюється, якщо вимірювальні прилади заключені в сталеві екрановані труби, які заземлені на кінцях. Сталеві труби є майже ідеальним екраном, оскільки силові лінії поля не досягають оболонок кабелів, а закінчуються на заземленій трубі. Екранування змінного магнітного поля засноване на протіканні струму в петлі, яка утворена заземленою на кінцях трубою і землею. Електромагнітне поле цього струму компенсує зовнішнє поле.

Зміщення потенціалу в імпульсному генераторі поряд з наведеними та індукованими ЕРС є суттєвими причинами появи завад. На рис.7.а; б приведені контури високої напруги, які складаються з генератора **Г** і об`єкта випробувань **Н** (де: **$Z_З$** – опір землі). Між елементами

пристрою, що знаходиться під високим потенціалом і заземленими предметами, існують паразитні ємності $\mathbf{C_П}$, які при імпульсних процесах швидко заряджаються і розряджаються. Внаслідок великих швидкостей зміни напруги, струми заряджання і розряджання повинні бути значними. Вони проходять через опір заземлення і створюють навіть на малих опорах землі значне зміщення потенціалу, а також вирівнювальні струми у всій системі заземлення. Якщо контур високої напруги знаходиться всередині клітки Фарадея (рис.7.б), то всі силові лінії закінчуються на екрані.

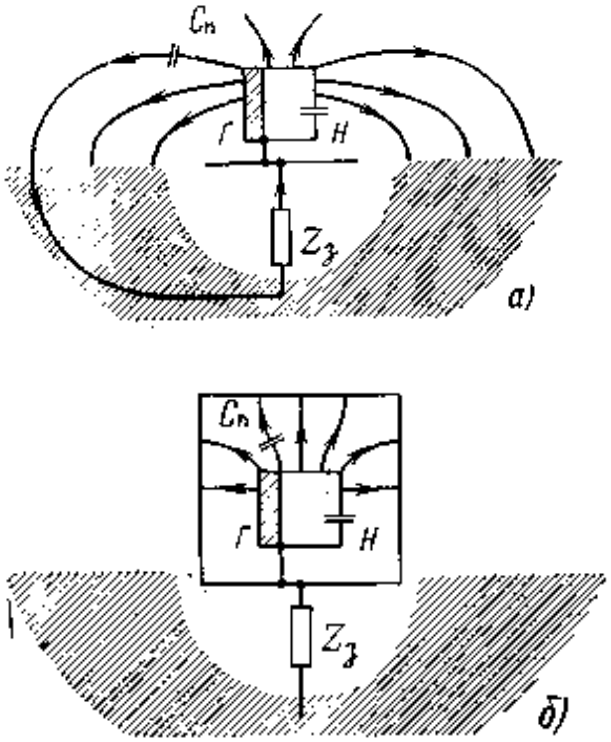


Рис.7. Зміщення потенціалу точки заземлення розрядного кола: (а) – картина силових ліній в звичайній електроустановці; (б) – те ж саме для електроустановки, яка розміщена в клітці Фарадея.

Струми протікають по внутрішній стінці клітки Фарадея і не можуть створити зміщення потенціалу на опорі землі. У цьому випадку не існує необхідності у використанні дуже малих опорів заземлення.

Рис.8. наглядно ілюструє виникнення зміщення потенціалу вздовж зворотнього провода, який прямує до імпульсного генератора.

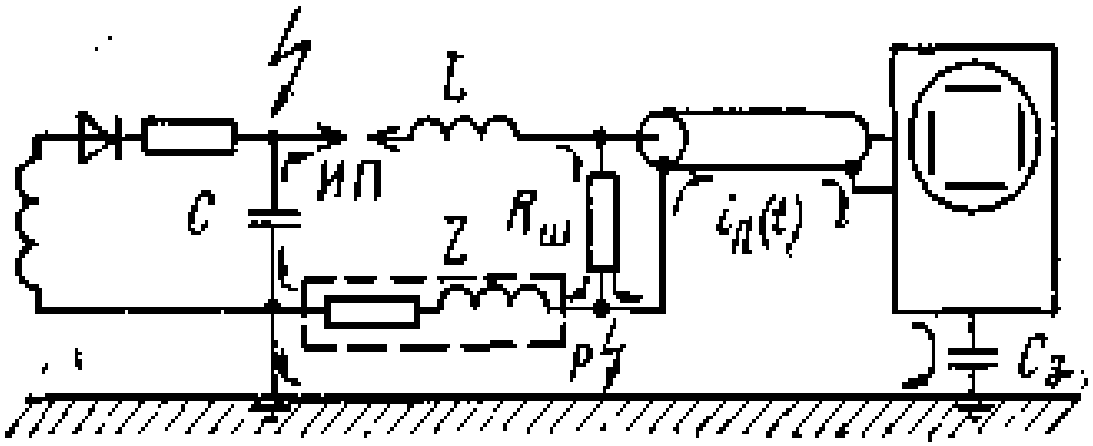


Рис.8. Схематичне представлення розрядного кола для пояснення виникнення завад за рахунок зміщення потенціалу на зворотньому проводі розрядного контуру при заземленому генераторі.

Після спрацювання іскрового проміжку «**ИР**» конденсатор «**С**» розряджається через індуктивність «**L**» і шунт «$\mathbf{R_{Ш}}$». В точці приєднання кабеля «**Р**» розрядний струм розгалуджується. Більша частина струму протікає назад до конденсатора безпосередньо по з`єднувальному провіднику. При цьому струм викликає спад напруги на зворотньому з`єднувальному провіднику з опором «**Z**», тому потенціал точки «**Р**» зміщується. Це зміщення потенціалу служить як ЕРС для струму в колі оболонки кабеля. Для ослаблення цього явища, рекомендується заземлювати імпульсний генератор не біля його основи, а в точці розгалудження «**Р**», тобто біля одного з виводів шунта (рис.9).

В цій схемі точка «Р» має потенціал землі, але зміщується приблизно на таку ж величину, що точка «**Р**» в схемі на рис.8. (потенціал нульового виводу конденсатора С).

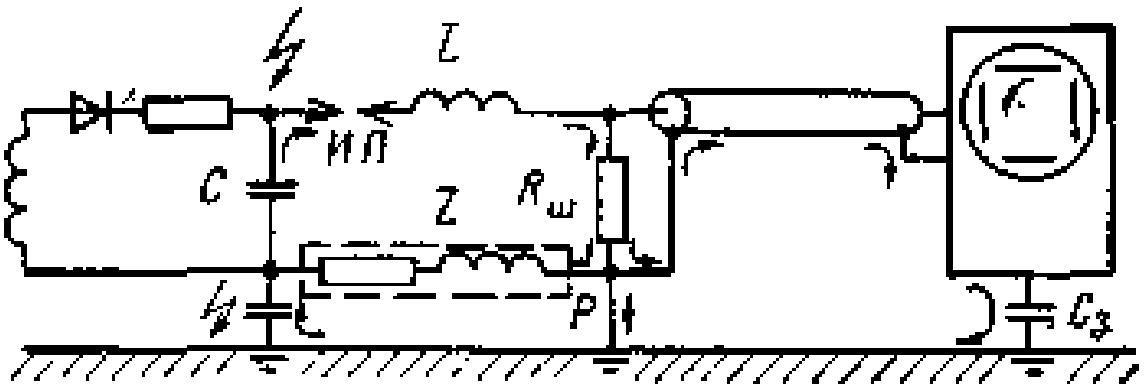


Рис.9. Схематичне представлення розрядного кола для пояснення виникнення завад за рахунок зміщення потенціалу на зворотньому проводі розрядного контура при заземленні з ш.унтом.

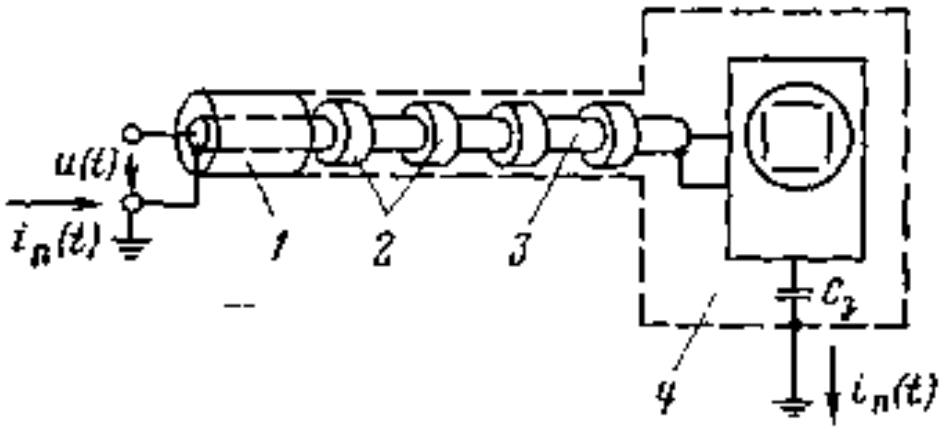


Рис.10. Схема пристрою з подавлення струму завад в оболонці кабеля та в корпусі: 1— мідний додатковий екран; 2 — ферритові сердечники; 3 — вимірювальний кабель; 4 — екранована кабінка.

Внаслідок наявності паразитних ємностей розрядного контура відносно землі також виникає **ЕРС**, викликає протікання струмів в оболонці кабеля. Очевидно, що існує оптимальний варіант виконання заземлення, при якому

струми в оболонках кабелів і по корпусам приладів порівняно малі. Проте зовсім її звести до нуля не вдається. Виходом з цього положення є конструювання пристрою за схемою, що наведена на рис.10; 11, при якому виключено протікання струмів довільної природи по оболонкам кабелів і корпусам приладів.

Внаслідок поверхневого ефекту, струм завади витісняється і протікає переважно по додатковому зовнішньому екрану та зовнішній поверхні екранованої кабінки.

Таким чином, він відводиться від оболонок кабеля і корпусу осцилографа. Зниження струму, що відгалуджується в оболонку кабеля досягається і за допомогою феритових сердечників, які одягаються на вимірювальний кабель (рис.11.). При цьому збільшується опір кола для струмів завад, що приводить до витіснення їх на зовнішній екран. Збільшення індуктивності в цих системах пропорційно квадрату числа витків. При цьому оболонка кабеля має мати зовнішню ізоляцію для виключення замикання між окремими витками кабеля і знеження міжвиткової ємності. При великій довжині кабеля стає помітним вплив розподілу напруги по оболонці кабеля. В таких випадках один концентрований намотаний кабелем дросель має не дуже широку смугу запирання. При деяких частотах вузли струму формуються в місцях приєднання дроселя. Тому необхідно струми в оболонці, довжина хвилі яких менша довжини кабеля, ослабити шляхом розподіленого за довжиною кабеля вмикання системи дроселів.

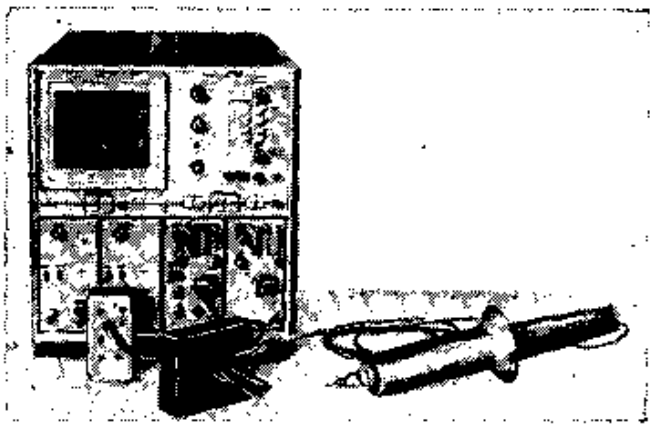


Рис.11. Подавлення струмів завад в оболонці кабеля і корпусі шляхом намотки вимірювального кабеля на сердечник з магнітом`ягкого матеріалу.

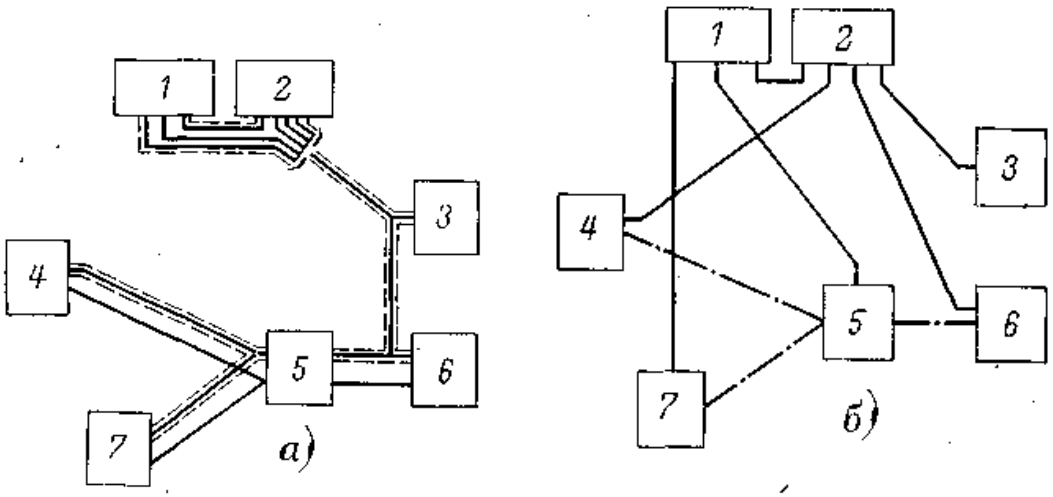


Рис.12. Схема з`єднань в імпульсних або ВЧ – пристроях. (а) раціональне розміщення проводів кола керування та вимірювальних кабелів; (б) неправильне розташування вимірювальних і керувальних проводів: 1 – прилад для вимірювання імпульсної напруги, 2 – пульт керування, 3 – випрямляч високої напруги, 4 – вимірювальний розрядник. 5 – дільник напруги. 6 – генератор імпульсної напруги, 7 – об`єкт випробування.

Рекомендовано прокладувати вимірювальні провідники за межами екранів в сталевих трубах, які прокладені за сіткою, що екранує приміщення. На рис.12.б. наведена принципова схема імпульсного пристрою, в якій можна чекати на неконтрольовані зміщення потенціалу і появу сильних завад. На рис.12.а. приведена рекомендована схема такого пристрою. У ньому всі провідники прокладені скритно в кабельних каналах. Воні всі не пересікаються між собою, а лише розгалуджуються.

4.Завдання лабораторної роботи.

4.1. Ознайомитись з основними методами екранування джерел імпульсних та високочастотних електромагнітних сигналів.

4.2. Розробити схему екранування приміщення з площею 4х 6 $м^2$ в якій розміщено інформаційно-комунікаційну систем (ІКС) призначену для обробки конфіденційної інформації і яка містить: два ком`ютери, 1 ксерокс та 1 принтер.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що вирішує задача екранування приміщення з **ІКС** та її елементів ?
2. Загальні вимоги до екранів приміщень.
3. Мережеві фільтри: призначення, схеми. Принцип роботи.
4. Охарактеризуйте причини появи завад від імпульсних та високочастотних пристроїв.
5. Індукована та наведена електрорушійна сила в системах заземлення та екранування.
6. Зміщення потенціалу в розрядних колах з імпульсними чи високочастотними джерелами.
7. Рекомендована схема сполучення системи імпульсних чи високочастотних пристроів **ІКС**.

<u>ТЕМА-8.</u> ВИВЧЕННЯ ЗАХИСНОГО ЗАЗЕМЛЕННЯ ПРИСТРОЇВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

1. Мета роботи.

Ознайомлення з основами технічного захисту середовища розташування інформаційно-комунікаційної системи та передавання з неї інформації через системи захисного заземлення.

Усвідомити значення захисного заземлення інформаційно-комунікаційних систем, засвоїти основи розрахунку захисного заземлення та ознайомитися з його типовими конструкціями.

2. Необхідні матеріали.

1. А. Шваб Измерения на высоком напряжении: Измерительные приборы и способы измерения. Перевод с немецкого. –М.: Энергоатомиздат. 1983. С. 23-32 (264с.).
2. О.К. Шуаібов Практикум з охорони праці. Навчальний посібник. –У.: Видавництво ДВНЗ «УжНУ» «Говерла». 2008. – 279 с.

Основні теоретичні відомості.

3.3. Загальні відомості про захисне заземлення

Однією з найважливіших умов захисту технічних засобів передавання інформації є правильне заземлення відповідних пристроїв. На практиці основною виступає радіальна система заземлення, яка має менше загальних ділянок для протікання сигнальних і живильних струмів у зворотному напрямку. Шина заземлення і заземлюючий контур не повинні мати петель, а мають виконуватися у вигляді розгалуженого дерева, де опір контуру не перевищує 1 Ом. Найчастіше в системах заземлення застосовуються вертикально занурені в землю сталеві труби довжиною 2-3 метри діаметром 35-50 мм. Труби дозволяють досягати

вологих шарів землі з найбільшою провідністю, які не піддаються висиханню чи промерзанню.

Опір заземлення визначається головним чином опором розтікання струму в землі. Його величину можна значно знизити за рахунок зменшення перехідного опору (опору між заземлювачем і грунтом) шляхом ретельного очищення поверхні труби від бруду та іржі, підсипанням у лунку по всій її висоті повареної солі і трамбуванням ґрунту навколо кожної труби. Заземлювачі (труби) варто з'єднувати між собою шинами за допомогою зварювання. Перетин шин і магістралей заземлення заради досягнення механічної міцності і одержання достатньої провідності рекомендується брати не меншим за 24х4 мм.

Магістралі заземлення поза будинком слід прокладати на глибині близько 1,5 метра, а всередині будинку - стінами або в спеціальних каналах, аби можна було їх регулярно оглядати. З'єднують магістралі з заземлювачами тільки за допомогою зварювання, а до технічних засобів передавання інформації магістраль підключають болтовим з'єднанням в одній точці. У випадку ввімкнення до магістралі заземлення декількох технічних засобів передавання інформації з'єднувати їх із магістраллю потрібно паралельно (при послідовному з'єднанні вимкнення одного з технічних засобів передавання інформації може призвести до вимкнення всіх інших). За пристрої заземлення не можна застосовувати природні заземлювачі: металеві конструкції будинків, які мають з'єднання з землею, прокладені в землі металеві труби, металеві оболонки підземних кабелів тощо.

Металеві неструмоведучі частини електрообладнання і електроустановок при порушенні ізоляції між ними і їхніми струмоведучими частинами можуть опинитись під напругою. У таких аварійних умовах дотик до неструмоведучих частин установок рівнозначний дотику до струмоведучих частин.

Усунення небезпеки ураження електричним струмом при такому переході напруги на неструмоведучі частини електроустановок у мережах з ізольованою нейтраллю здійснюється за допомогою захисного заземлення (рис.1).

Під ***захисним заземленням*** розуміють з'єднання металевих неструмоведучих частин електроустановок з землею через заземлюючі провідники і заземлювачі для створення між цими частинами і землею малого опору.

Найпоширеніший і найнадійніший засіб електрозахисту - захисне заземлення. Воно базується на зменшенні до безпечних значень напруги дотику і крокової напруги. Цього досягають шляхом зменшення опору заземлення.

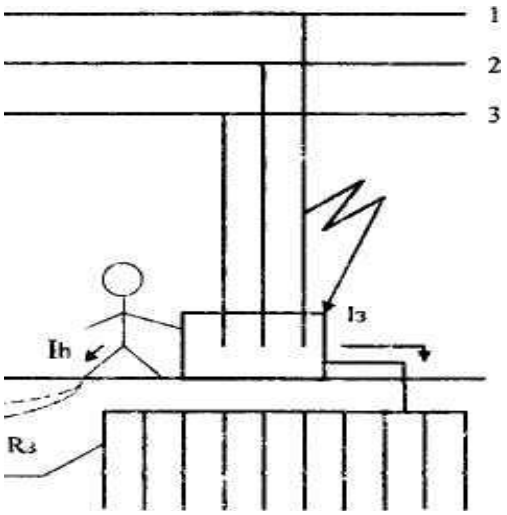


Рис.1. Принципова схема захисного заземлення

Захисне заземлення влаштовують у трифазних мережах із заземленою нейтраллю та напругою до 1000 В, а вище 1000 В - за будь-якого режиму роботи нейтралі. Заземленню підлягають електроустановки напругою вище за 42 В змінного струму у приміщеннях із підвищеною небезпекою та особливо небезпечних, а також у зовнішніх установках.

Ручні електрифіковані інструменти, що працюють із напругою вище 42 В, підключають у мережу через штепсельні розетки, які, крім фазних контактів, мають і заземлювальний контакт. Штепсельні з'єднання виконані так, що під час вмикання заземлюючий контакт входить раніше фазних контактів, за рахунок чого гарантується безпека при обслуговуванні електрообладнання. Заземлюючий контакт довший за фазні, що виключає помилкове вмикання.

У контурних заземлювальних пристроях заземлювачі розташовують по контуру (периметру) будівлі, у якій знаходиться електрообладнання, яке потрібно заземлити (рис.2. а).

У місцях із високим питомим опором грунту економічно може бути більш доцільним улаштування виносних заземлювачів, які розміщують у більш провідних шарах землі (рис.2. *б).*

При виникненні замикання на корпус споживача електричного струму із фаз мережі через заземлюючий пристрій починає протікати струм замикання ($I_з$), викликаний наявністю опорів ізоляції фаз мережі і ємностей фаз відносно землі.

Частина цього струму I_h відгалужується на тіло людини, яка торкається металевих неструмоведучих частин електроустановки. Величина цього струму залежить від величини струму замикання на землю $I_З$, опору розтікання струму в землі заземлюючого пристрою $R_З$, повного опору в колі «людина-земля» R_{ch}, взаємного розташування електрообладнання, заземлюючого пристрою, яке враховується коефіцієнтом напруги дотику $\alpha \leq 1$ і визначається за формулою:

$$I_h = I_a R_З \alpha / R_{ch}, \qquad (1)$$

Повний опір у колі «людина-земля» складається із опору людини R_h, опору взуття $R_{ВЗ}$ і опору розтікання струму від підошви взуття в землю $R_{ПЗ}$ і визначається за виразом:

$$R_{ch} = R_h + R_{ВЗ} + R_{ПЗ}, \qquad (2)$$

Якщо людина не має спеціального діелектричного взуття і стоїть на струмопровідній підлозі чи землі, то можна вважати, що $R_{ВЗ} = 0$, $R_{ПЗ} = 0$ і $R_{ch} = R_h$.

Розрізняють штучні і природні заземлювачі. В якості природних заземлювачів можна використовувати різні металоконструкції, які добре контактують з землею:

арматуру залізобетонних конструкцій, трубопроводи (за виключенням тих, що використовуються для транспортування горючих і вибухових рідин або газів), металеві оболонки кабелів (але не алюмінієві) та інші конструкції. Штучними заземлювачами є спеціально влаштовані металоконструкції.

Характеристики стаціонарних заземлювачів та струмовідводів приведені в таблиці 1.

Опір розтіканню струму з одного заземлювача (труби, стержня) залежить від питомого опору грунту, глибини від поверхні землі до верху заземлювача і розмірів самого заземлювача. Цей опір можна розрахувати за формулою:

$$R_{mp} = 0.366\ \rho/l\ [\lg(2l/d) + 0.5\ 1g(4t + l)/(4t-l)], \quad (3)$$

де ρ- питомий опір грунту, Ом • м; l - довжина заземлювача, м; *d* - діаметр заземлювача, м; t - відстань від поверхні землі до середини вертикального заземлювача, м (рис.5.2); $t = h_в + l/2$, де $h_в$ — глибина викопаної траншеї, у яку вбивають вертикальні заземлювачі, м (рис.2).

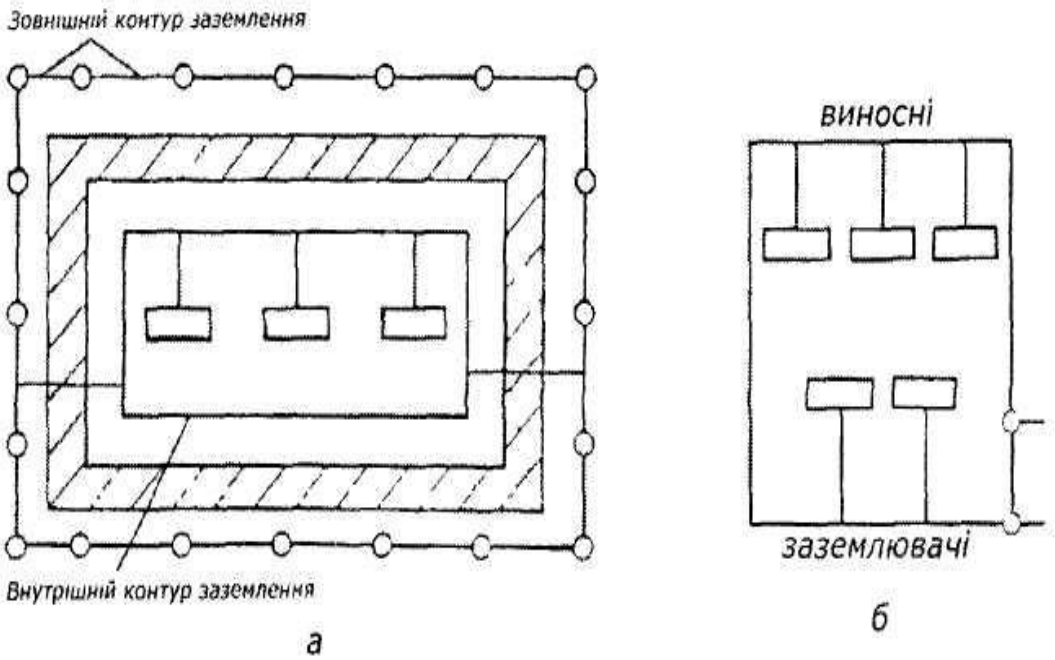


Рис.2. Принципова схема контурного і виносного заземлення

Конструкції типових заземлювачів представлені на рис.3.

Питомий опір ґрунту залежить від його будови, вмісту в ньому розчинних речовин, вологи, а також від температури повітря. Він змінюється сезонно, а відтак сезонно змінюється і значення опору розтіканню струму заземлювальної системи.

Питомий електричний опір грунту залежить від його структури, вологості, температури, затверділості й пори року (табл.2).

Питомий електричний опір ґрунту з урахуванням коефіцієнта сезонності визначається за співвідношенням:

$$\rho = \rho_B \, \eta_C \, , \qquad (4)$$

де -ρ_B - вимірювальний питомий електричний опір, Ом•м;
η_C - коефіцієнт сезонності.

Коефіцієнт сезонності залежить від вологості землі при вимірюванні (табл.3).

Групове розташування вертикальних заземлювачів (труб) спричиняє взаємний вплив полів розтікання (екранування) струму, збільшуючи опір розтіканню струму.

Ураховуючи коефіцієнт екранування, отримаємо:

$$R_\rho = R_{mp}/(n \, \eta_C), \qquad (5)$$

де R_{mp}- опір розтіканню струму одного заземлювача, Ом•м; n - кількість заземлювачів, шт.; η_C - коефіцієнт екранування.

Значення коефіцієнта екранування вертикальних заземлювачів для контурного заземлення подано у табл.4.

З урахуванням коефіцієнтів сезонності та екранування кількість заземлювачів (труб) визначається за формулою:

$$n = R_{mp}/(R_д \, \eta_C \, \eta_e), \qquad (6)$$

де $R_{тр}$ - опір одного заземлювача, Ом; $R_д$ = 4 Ом - припустимий опір розтікання струму заземлення.

Таблиця 1.

Основні характеристики заземлювачів і струмопроводів

Струмовідводи та заземлювачі	**Назва**	**Характеристика**
Струмовідводи	Заземлення верстатів, машин, металевої апаратури резервуарів, котлів, трубопроводів	Сталева стрічка перерізом 48 мм^2, завтовшки більш як 4 мм
	Заземлення гумових шлангів і лійок	Гнучкий сталевий провід перерізом не менш ніж 12 мм^2
Заземлювачі	Заземлювальний контур зі сталевих труб (електродів)	Труби діаметром 38 60 мм, із товщиною стінки понад 3.5 мм. Сталеві стержні діаметром 40 50 мм, завдовжки 2 3м. Вбивають вертикальні заземлювачі в землю на глибину від поверхні землі до верху труби або стержня 0.6 0.8 м.
Сталеві стрічки	Для струмовідводів (електродів)	Перерізом не менш ніж 100 мм', завтовшки не менш ніж 4 5 мм, заглиблюють в землю на глибину 0,6 0,8 м
Сталеві пластини	Для струмовідводів (електродів)	Товщина не менш є 4 мм і площа не менш ніж 1 м Заглиблюють у землю вертикально на глибину від поверхні землі до пластини

Таблиця 2.

Питомий електричний опір ґрунту

Ґрунт	Питомий електричний опір, Ом м	
	Границя зміни	**При вологості 10...20 %**
Чорнозем	**9...53**	20
Глина	**8...70**	40
Суглинок	**40...**150	100
Пісок	400...700	700
Супісок	150...400	300

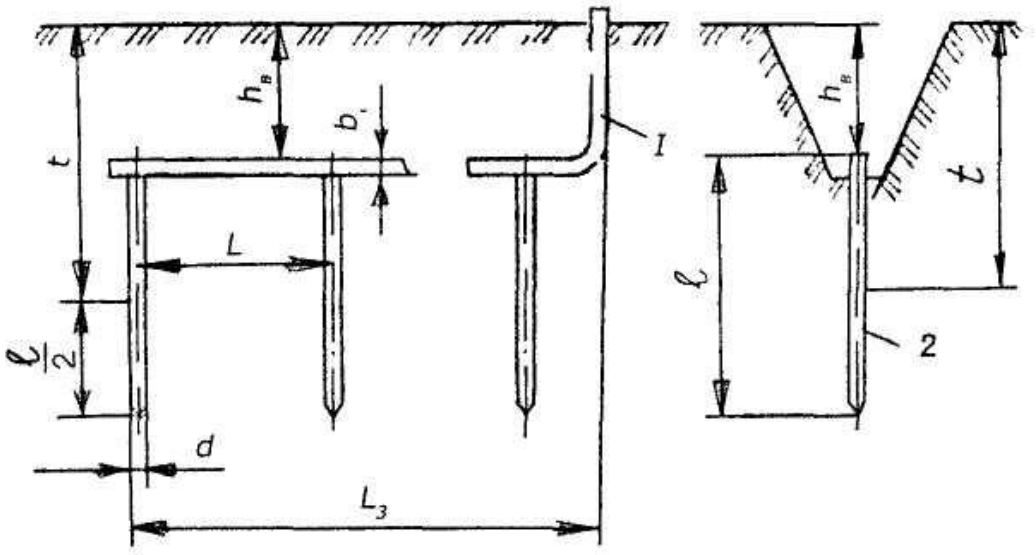


Рис.3. Схема розміщення заземлювачів групового заземлення:1 - з'єднувальна стрічка; 2 - заземлювач (труба); h_e - глибина закладання заземлювачів; L - відстань між заземлювачами; t - відстань від середини заземлювача до поверхні грунту; l - довжина заземлювача (стержня або труби); b - ширина з'єднувальної стрічки.

Таблиця 3.

Значення коефіцієнта сезонності для вертикального заземлювача та горизонтальної стрічки

Вологість землі при вимірюванні		
підвищена	нормальна	мала
η_C для вертикального електрода		l = 3 м
1.9	1.7	1.5
1.7	1.5	1.3
1.5	1.3	1.2
1.3	1.1	1.0
η_C для горизонтального електрода		l = 10 м
9.3 5.9 4.0 2.5	5.5 3.5 2.5 1.5	4.1 2.5 2.0 1.1
η_C для горизонт 7.2 4.8 3.2 2.2	ального електрода 4.5 3.0 2.0	l = 50 м 3.6 2.4 1.6 1.ё12

Таблиця 4

Значення коефіцієнта екранування

Відношення віддалі до довжини електрода, *L/l*	Число заземлювачів (труб)				
	4	6	10	20	40
1	0.66-0.72	0.58-0.65	0.52-0,58	0.44-0.50	0.38-0.44
1	0.76-0.80	0.71-0.75	0.66-0.71	0.61-0.66	0.55-0.61
3	0-83-0.86	0.78-0.82	0.74-0.78	0.68-0.73	0.64-0.69

Довжину з'єднувальної стрічки визначають за формулою:

$$l_{стр} = 1.05\ L\ (n-1), \qquad (7)$$

де *L* - відстань між заземлювачами, м.

Опір розтіканню струму в з'єднувальній стрічці можна розрахувати за виразом:

$$R_{стр} = 0.366\ (\rho/l_{стр})\ lg(2\ l^2_{стр})/(h\ b\ \eta_{стр}), \qquad (7.8)$$

де ρ - питомий електричний опір грунту з урахуванням коефіцієнта сезонності, Ом • м; l - довжина з'єднувальної стрічки, м; *h* - глибина (траншеї) закладання з'єднувальної стрічки, м; *b* - ширина з'єднувальної стрічки, м; $\eta_{стр}$ - коефіцієнт екранування з'єднувальної стрічки.

Коефіцієнт екранування з'єднувальної стрічки для контурного заземлення приймають залежно від кількості заземлювачів (табл.5).

Загальний опір розтіканню струму заземлювачів та стрічки, що з'єднує визначається за формулою:

$$R_З = (1/R_{тр} + 1/R_{стр})^{-1} \le R_д \qquad (9)$$

Таблиця 5.

Значення коефіцієнта екранування для контурного заземлення

Відношення віддалі електрода (труби) до довжини електрода, *L/I*	Число заземлювачів (труб)				
	4	6	10	20	40
1	0,45	0,40	0,34	0,27	0,23
2	0,55	0,48	0,40	0,32	0,25
3	0,70	0,64	0,56	0,45	0,40

3.4. Розрахунок захисного заземлення методом коефіцієнтів використання

Вихідними даними для розрахунку є: допустимий опір розтікання струму землі заземлюючого пристрою $R_{З.норм}$. (табл.6); питомий опір грунту в місці спорудження заземлювача ($\rho_З$, Ом*м); тип заземлювача і його конструктивні розміри, м; конструкція заземлюючого пристрою (заземлювачі розташовані в ряд чи по периметру).

Розрахунок захисного заземлення здійснюється методом коефіцієнтів використання електродів при однорідній структурі грунту для розрахунку простих заземлюючих пристроїв.

Нижче наведений порядок розрахунку заземлюючих пристроїв в однорідній землі за методом коефіцієнтів використання.

Метою подібних розрахунків захисного заземлення є визначення кількості електродів заземлення і заземлюючих провідників, їхніх розмірів і схеми розміщення в грунті, При цьому, опір заземлюючого пристрою чи напруга дотику при замиканні фази на заземлені частини електроустановок не повинні перевищувати допустимі значення.

Розлянемо основні елементи розрахунку.

1. Визначають розрахунковий питомий опір землі $\rho = ф*\rho_з$, де ф - коефіцієнт сезонності, який враховує можливі коливання питомого опору землі при зміні вологості землі протягом року (табл.7).
2. Визначають опір розтікання струму в землі одного вертикального заземлювача заглибленого на величину h (рис. 2) від поверхні землі за формулою:

$$R_В = (\rho_{р.З}/2\pi L[\ln(2L/d)+(l/2)\ln((4t+l)/(4t-1)], \qquad (10)$$

де $R_В$ - опір розтікання струму в землі вертикального заземлювача;

$\rho_{р.З}$ - розрахунковий питомий опір землі, Ом*м;

L - довжина заземлювача, м;

d - діаметр заземлювача (для кутникової сталі) d = 0.95b, де b - ширина полки кутника, м;

t - віддаль від поверхні землі до середини заземлювача, м.

Таблиця.6

Допустиме значення опору захисного заземлення в електротехнічних установках

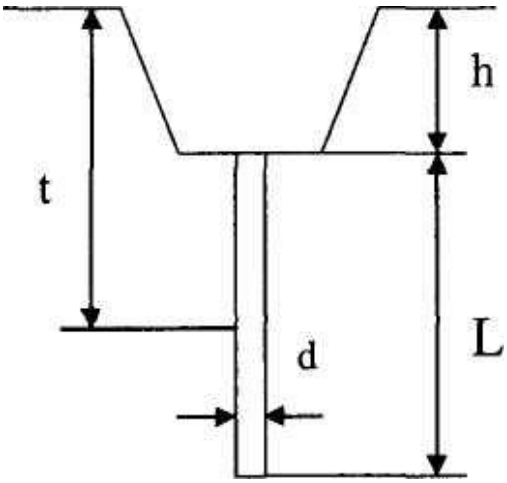
Характеристика установок	Найбільший допустимий опір заземлення, Ом
Установки напругою вище 1000 В	
Захисне заземлення в установках з великими струмами замикання на землю (I_3 > 500 А)	0,5
Захисне заземлення в установках з малими струмами замикання на землю (I_3 < 500 А), заземлюючий пристрій одночасно використовується для установок напругою до 1000 В заземлюючий пристрій використовується тільки для установок напругою вище 1000 В	125/U < Ю 250/Із < Ю
Установки напругою до 1000 В	
Захисне заземлення всіх установок	4

Таблиця 7

Характеристики кліматичних районів, наближені значення поправочних коефіцієнтів ф до величини р

Характеристика районів і види заземлювачів, які застосовуються	Райони			
Середня багаторічна нижча температура (січень) °С	-20: -15	-14: -10	-10: 0	0: +5

Середня багаторічна вища температура (липень) °С	15-18	18-22	22-24	24-26
Тривалість замерзання вод. Днів.	190-170	"150	"100	0
Види заземлювачів і поправочні коефіцієнти ф до величини p_3				
Стержневі заземлювачі (кутникова сталь, труби) довж. 2-3 м при глибині закладання від вершини 0,5-0,8 м	1.65	1.45	1.3	1.1
Заземлювачі великої довжини (смуга, кругла сталь), довжиною 10 м при глибині закладання 0.8 м	5.5	3.5	2.5	1.5



h - глибина розташування заземлювача в грунті, м;
L - довжина заземлювача, м;
d - діаметр заземлювача, м;
і - віддаль від поверхні грунту до середини заземлювача, м.

Рис.5. Схема розташування вертикального заземлювача в грунті.

3. Визначаємо орієнтовну кількість вертикальних заземлювачів n*:

$$n^* = R_B/R_{З.НОРМ}., \quad (11)$$

4. Визначають з таблиць 8 або 9 коефіцієнт використання заземлювачів $\eta_в$, що враховує ефект екранування при вибраному значенні $K=\alpha/1$, де η- віддаль між заземлювачами, м; l -довжина заземлювача, м (К може бути вибране рівним 1, 2 або 3).
5. Визначають кількість заземлювачів n з урахуванням $\eta_В$ за формулою:

$$n = R_В/(R_{З.НОРМ} *\eta_В). \quad (12)$$

6. Знаходять довжину горизонтального заземлювача L, яка з'єднує вертикальні заземлювачі, за формулами:
   L= a (n-1) - розташованих у ряд, м;
   L = a * n - розташованих по контуру, м.
7. Визначають опір горизонтального заземлювача $R_г$, прокладеного на глибині h від поверхні землі, за формулою:

$$R_Г = (\rho_{р.З}/2\pi L)*\ln(2L^2/(b*h), \quad (13)$$

де $R_г$ - опір розтікання струму в землі горизонтального заземлювача, Ом;
L - довжина горизонтального заземлювача, м;
b - ширина смугової сталі, з якої виготовлено заземлювач;
h - глибина розташування горизонтального заземлювача, м.

8. Обчислюють загальний опір заземлюючого пристрою за формулою:

$$R_З = R_В*R_г/(n*R_г*\eta_в + R_г*\eta_в), \quad (14)$$

де $R_З$ - загальний опір заземлюючого пристрою, Ом; $\eta_в$ - коефіцієнт використання горизонтального заземлювача, який визначають з табл.5 або 6.

Отримане значення опору штучного заземлення не повинно перевищувати допустиме значення оперу захисного заземлення

Таблиця 8

Коефіцієнт використання вертикальних електродів $\eta_в$ з кутникової сталі або труб, які розміщені в ряд (без врахування впливу смуги з'єднання)

Число електродів	Відношення віддалі між електродами до довжини		
		2	3
2	0.84 - 0.87	0.9 - 0.92	0.93 - 0.95
3	0.76 - 0.8	0.85 - 0.88	0.9 - 0.92
5	0.67 - 0.72	0.79 - 0.83	0.85 - 0.88
10	0.56 - 0.62	0.72 - 0.77	0.79 - 0.83
15	0.51 - 0.56	0.66 - 0.73	0.76 - 0.8
20	0.47 - 0.5	0.65 - 0.7	0.74 - 0.79

Таблиця 9

Коефіцієнт використання вертикальних електродів $\eta_в$ з кутникової сталі або труб, розміщених по контуру (без врахування впливу смуги з'єднання)

Число електродів	Відношення віддалі між електродами до довжини		
	1	2	3
2	0.84- 0.87	0.9 - 0.92	0.93 - 0.95
3	0.6 - 0.8	0.85 - 0.88	0.9 - 0.92
5	067 - 0.72	0.79 - 0.83	0.85 - 0.88
10	0.56 - 0.62	0.72 - 0.77	0.79 - 083
15	0.51 - 0.56	0.66 - 0.73	0.76 - 0.8
20	0.47 - 0.5	0.65 - 0.7	0.74 - 0.79

Таблиця 10

Коефіцієнт використання горизонтального заземлювача $\eta_г$, який з'єднує вертикальні заземлювачі при їх розташуванні в ряд

Відношення віддалі між електродами до довжини електрода	Число електродів в ряді			
	4	10	20	30
1	0.77	0.62	0.42	0.31
2	0.89	0.75	0.56	0.46
3	0.92	0.82	0.68	0.58

Таблиця 11

Коефіцієнти використання горизонтального заземлювача $Г|_г$,
який з'єднує вертикальні заземлювачі
при їх розташуванні по контуру

Відношення віддалі між електродами до довжини електрода	Число електродів в контурі					
	4	10	20	30	50	70
1	0.45	0.34	0.27	0.24	0.21	0.20
2	0.55	0.40	0.32	0.30	0.28	0.26
3	0.70	0.56	0.45	0.41	0.37	0.35

4.Завдання лабораторної роботи.

4.1. Ознайомись з основами розрахунку захисного заземлення. Спроектувати і розрахувати систему захисного заземлення для ІКС, описану в п.4.1., у якої опір заземлення буде знаходитись в межах 0,5-0,3 Ом. Розрахунок заземлення провести методом коефіцієнтів використання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Охарактеризуйте принципову схему захисного заземлення та умови її застосування.
2. Від яких чинників залежить струм замикання на землю і повний опір в колі «людина-земля» ?
3. Від яких параметрів і як залежить опір одиничного заземлювача ?
4. Охарактеризуйте принципову схему контурного і виносного заземлення. Як визначити питомий опір грунту ?
5. Стаціонарні заземлювачі і струмовідводи та коефіцієнт сезонності (чинники від яких він залежить).
6. Як визначити кількість заземлювачів з урахуванням коефіцієнтів сезонності і екранування ?
7. Охарактеризуйте коефіцієнти екранування контурного заземлення.
8. Повний опір заземлювачів і з’єднувальної стрічки ?
9. Коли розрахунок захисного заземлення слід проводити методом коефіцієнтів використання ?
10. Допустимі значення опору захисного заземлення в електроустановках.
11. Методика розрахунку захисного заземлення методом коефіцієнтів використання ?

6. Питання модульних контролів.

МОДУЛЬ-1

1. Основні проблеми інформаційної безпеки і базові принципи створення системи безпеки інформації в Україні.
2. Що складає загрози інформаційній безпеці України.
3. Сформулюйте основні концептуальні питання інформаційної безпеки України.
4. Концепція технічного захисту інформації в Україні. 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. Наведіть базові принципи, які адекватно відображають сутність захисту інформації в країнах **НАТО** та **ЄС**.
8. Охарактеризуйте ступені секретності інформації в країнах **НАТО** і **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 визначає модель порушника?
13. Наведіть загальні відомості про політику безпеки та охарактеризуйте основні принципи, покладені в основу політики інформаційної безпеки.
14. Основні кроки розроблення політики безпеки.
15. Організація виконання відновлювальних робіт і забезпечення неперервного функціонування автоматизованої системи (**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 план здійснення державної експертизи.
21. Охарактеризуйте процедуру і основні етапи сертифікації засобів технічного зазисту інформації.
22. Основні етапи проведення технічного захисту інформації в Україні. Які шляхи здійснення загроз безпеці інформаці Вам 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 та здійснення первинних технічних заходів захисту інформації
25. Дайте визначення терміну «***інформація з обмеженим доступом***». У яких випадках інформація 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 державної, 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 забезпечення захисту інформації. Права і основні функці служби захисту інформації (**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 основні 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 містилась.
44. 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.

МОДУЛЬ-2

1. Визначення і термінологія в сфері захисту інформації у автоматизованих системах.
2. Охарактеризуйте об`єкт і суб`єкт захисту інформації згідно Закона України «***Про захист інформації в автоматизованих системах***» (від 5 липня 1994 р.).
3. В чому полягають особливості відносин між власником інформації, власником автоматизованої системи та її користувачем (стаття 5 ЗУ «***Про захист інформації в автоматизованих системах***» (від 5 липня 1994 р.).
4. Охарактеризуйте забезпечення захисту інформації в автоматизованих системах та умов її обробки (статті 8 і 9 **ЗУ** «***Про захист інформації в автоматизованих системах***» (від 5 липня 1994 р.).
5. Наведіть класифікацію та перелік основних загроз безпеці інформаційних систем.
6. Дайте класифікацію атак на інформаційно-комунікаційну систему.
7. Наведіть основні положення моделі загроз безпеці інформації.
8. Які об`єкти інформаційної діяльності підлягають категорюванню?
9. Якою є мета категорювання об`єктів інформаційної діяльності?
10. Які об`єкти інформаційної діяльності Підприємства відносяться да I, II. III і IV категорій?
11. Охарактеризуйте порядок надання категорій об`єктам інформаційної діяльності.
12. Засекречування та розсекречування матеріальних носіїв інформації та звід відомостей, що становлять державну таємницю.
13. Дайте характеристику термінів «**порушник**» і «**хакер**».
14. В чому проявляються наслідки від дій порушників інформаційної безпеки?
15. Охарактеризуйте модель порушника.
16. Охарактеризуйте структуру системи захисту інформації та її рівні.
17. Функціональні сервіси безпеки і механізми, що їх реалізують.
18. Таксономія функцій систем захисту інформації.
19. Механізми захисту інформації на різних рівнях інформаційно-комунікаційних систем.
20. Загальна характеристика коплексу засобів захисту.

21. Підсистема забезпечення цілісності та криптографічна система Підпрємства.
22. Підсистеми ідентифікації, автентифікації та керування доступом до інформації.
23. Охарактеризуйте можливості системи електронного конфіденційного документообігу.
24. Наведіть технічні можливості системи конфіденційного електронного сховища.
25. Охарактеризуйте будову системи сполучення електронного і паперового діловодства.
26. Будова і рубежі захисту системи електронного конфіденційного діловодства.
27. Охарактеризуйте можливості технічних засобів захисту електронного діловодства.
28. Аудит безпеки інформаційних систем.
29. Зміст і послідовність робіт з протидії загрозам системі захисту інформації.
30. Які технічні засоби захисту інформації відносяться до основних, а які до домоміжних?
31. Охарактеризуйте зміст роботи із захисту інформації від витоку технічними каналами.
32. В чому полягають організаційні заходи із захисту інформації від витоку технічними каналами?
33. Підгготовчі та основні технічні заходи із захисту інформації від витоку технічними каналами.
34. Основні елементи захисту інформації при застосуванні копіювальної і розмножувальної техніки.
35. Вимоги і організація технічного захисту інформації при застосуванні копіювальної і розмножувальної техніки.
36. Рекомендації щодо захисту інформації, яка обробляється засобами копіювально-розмножувальної техніки класу «Б».
37. Охарактеризуйте класифікатор засобів копіювально-розмножувальної техніки.
38. Наведіть загальні положення із захисту інформації в комп`ютерній системі Підприємства та основні загрози цій інформації.
39. Охарактеризуйте обчислювальну підсистему комп`ютерної системи Підприємства.
40. Алгоритм захисту інформації в комп`ютерній системі Підприємства від витоку технцічними каналами.
41. Рекомендації відносно захисту інформації в комп`ютерній системі Підприємства від перехоплень різних фізичних чиннків.

42. Характеристики фізичного середовища комп`ютерної системи Підприємства.
43. Характеристика користувачів комп`ютерної системи Підприємства.
44. Характеристика опрацьованої в комп`ютерній системі інформації та технології роботи з нею.
45. .Категорії засобів технічного захисту.
46. Охоронна і пожежна сигналізації Підприємства.
47. Охоронне телебачення.
48. Заземлення – як технічний засіб передавання інформації.
49. Мережеві фільтри в системах передавання інформації.
50. Екранування приміщень – як спосіб технічного захисту передавання інформації.
51. Способи виявлення незаконних підключень до мереж передачі інформації.
52. Охарактеризуйте умови праці персоналу при роботі з відеодисплейними системами і комп`ютерами.
53. Дайте характеристику впливу електромагнітних полів на здоров`я персоналу сучасних комп`ютерних систем.
54. Охарактеризуйте санітарні норми для електромагнітного випромінювання і захисту від нього працівників комп`ютерних систем.
55. Система «***Людина – комп`ютер – середовище***» та вимоги охорони праці до неї і приміщень з інформаційно-комунікаційними системами.

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.
10. А. Шваб Измерения на высоком напряжении: Измерительные приборы и способы измерения. Перевод с немецкого. –М.: Энергоатомиздат. 1983. С. 23-32.
11. В. Бегун, Горбунов О.В. Каденко И.Н и др. // Вероятностный анализ безопасности атомных станций. -Киев. -2000. - 563 с.
12. О.К. Шуаібов, І.Й. Росола Теоретичні основи та логічні моделі безпеки життєдіяльності. Ужгород. 2007. Видавництво УжНУ «Говерла». 307 с.

Навчально-методичний посібник:
Практикум з організаційно-технічного захисту інформації в інформаційно-комунікаційних системах.

Автор: професор **Шуаібов Олександр Камілович**

Навчально-методичний посібник для самостійної роботи студентів

Підписано до друку 2013 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-