Міністерство освіти і науки України
Національний університет водного господарства
та природокористування
Кафедра обчислювальної техніки

04-04-255М

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт з навчальної дисципліни
«Системи технічного захисту інформації»
для здобувачів вищої освіти другого (магістерського) рівня
галузі знань 12 «Інформаційні технології»
за спеціальністю 123 «Комп'ютерна інженерія»
денної та заочної форм навчання

Рекомендовано науково-
методичною радою
з якості ННІАКОТ
Протокол №7 від 29.05.2023 р.

Рівне – 2023

Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни «Системи технічного захисту інформації» для здобувачів вищої освіти другого (магістерського) рівня галузі знань 12 «Інформаційні технології» за спеціальністю 123 «Комп'ютерна інженерія» денної та заочної форм навчання [Електронне видання] / Назарук В. Д. – Рівне : НУВГП. – 47 с.

Укладач: Назарук В. Д., кандидат технічних наук, старший викладач кафедри обчислювальної техніки.

Відповідальний за випуск: Круліковський Б. Б., завідувач кафедри обчислювальної техніки.

Керівник (гарант) освітньої програми «Комп'ютерна інженерія» спеціальності 123 «Комп'ютерна інженерія» Круліковський Б. Б.

ЗМІСТ

Вступ

З ростом рівня інформатизації суспільства удосконалюються методи та засоби несанкціонованого доступу та впливу на інформацію, яка має важливе значення як для держави, так і для особистості. Це стосується всіх об'єктів інформаційної діяльності, де здійснюється створення, обробка та передача інформації.

Тому для належного захисту інформаційних ресурсів необхідно постійно оновлювати наукову і технічну базу розвитку відповідних засобів. Належних результатів можна досягнути при комплексному підході до застосування технічних та криптографічних методів захисту.

В ході вивчення теоретичної частини дисципліни «Системи технічного захисту інформації» та відпрацювання завдань лабораторного практикуму студенти зможуть освоїти:

- Порядок аналізу та локалізації несанкціонованого доступу до інформації в комп'ютерних системах;
- Виявлення та знешкодження каналів технічного витоку інформації на об'єктах інформаційної діяльності;
- Криптографічні методи захисту інформації.

Методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах визначено в нормативних і методологічних документах, регламентуючих питання технічного захисту інформації.

При проектуванні комп'ютерних систем застосування адекватних засобів захисту є обов'язковою складовою їх безпечного функціонування. Тому практичне застосування отриманих в процесі вивчення навчальної дисципліни «Основи теорії захисту інформації» має важливе значення і викладено у вигляді лабораторного практикуму.

Методичні вказівки до виконання лабораторних робіт надають студентам можливість набути практичних навичок впровадження апаратних та програмних комплексів засобів захисту в автоматизовані системи різних класів та категорій.

Дані методичні вказівки можуть бути корисними фахівцям установ, підприємств та організацій, які займаються питаннями захисту інформації на об'єктах інформаційної діяльності.

Загальні методичні вказівки

Лабораторні роботи спрямовані на відпрацювання студентами вмінь і навиків використання діючих комплексів засобів захисту об'єктів інформаційної діяльності та комп'ютерних систем від несанкціонованого доступу та перехоплення інформації за допомогою технічних засобів розвідки.

В якості умовного зразка комп'ютерної системи, для якої необхідно створювати КСЗІ, обирається автоматизована система класу 1 (АС класу 1), встановлена **в підрозділі кадрового забезпечення організації** (установи, підприємства), де студент працює, працював, або проходив практику. АС призначена для обробки інформації з обмеженим доступом, яка містить персональні дані співробітників організації.

Під час виконання лабораторних робіт використовуються та конкретизуються положення НД ТЗІ, які відповідають вимогам і умовам, притаманним для вищевказаної організації (АС).

Кожна лабораторна робота розрахована на 2 години лабораторних занять.

Звіт про кожну лабораторну роботу виконується в текстовому редакторі Word, зберігається окремим документом та надсилається на перевірку викладачу в навчальні платформі Moodle.

Лабораторна робота №1
Визначення амплітуди гармонік та побудова спектра побічних електромагнітних випромінювань монітора комп'ютера.

Мета роботи: Освоїти навики пошуку гармонік побічних електромагнітних випромінювань компонентів комп'ютера, призначеного для обробки інформації з обмеженим доступом.

Завдання лабораторної роботи: визначити амплітуди небезпечних сигналів випромінювання основної та бічних гармонік.

Для виконання лабораторної роботи використовується вимірювальний комплект, який складається з селективного мікровольтметра STV 301-2 та феритової стержневої антени FSA-101. Зовнішній вигляд та органи управління селективного мікровольтметра STV 301-2 зображені на рис. 1.1, зовнішній вигляд елементів антени зображено на рис.1.2.

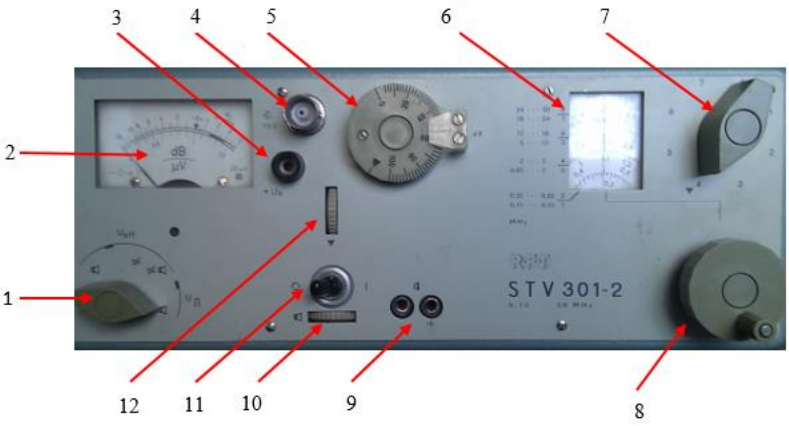

Рис. 1.1 Органи управління STV 301-2

Органи управління селективного мікровольтметра STV 301-2 позначені наступними позиціями:

1 – перемикач режимів роботи;

2 – індикатор приладу;

3 – гніздо під'єднання живлення антенного підсилювача;

4 – гніздо під’єднання антенного фідера;
5 – регулятор атенюатора;
6 – частотна шкала;
7 – перемикач діапазонів частот;
8 – ручка вибору частоти;
9 – гніздо підключення навушників;
10 – регулятор підсилювача гучномовця;
11 – тумблер електроживлення;
12 – регулятор калібрування.

1 Підготовка комплекту до роботи.

Селективний мікровольтметр поставити, звівши його на ручку-упор. За допомогою шнура під’єднати до мережі 220 В. та перевести тумблер 1.11 в праве положення.

1.1 Калібрування приладу.

Для калібрування необхідно регулятор атенюатора 1.5 поставити в положення ▼, перемикач режимів роботи 1.1 поставити в положення ▼. Не під’єднуючи фідер антени, регулятором калібрування 1.12 встановити стрілку індикатора приладу в положення «0».

1.2 Встановлення приймальної частоти.

За допомогою перемикача діапазонів частот (7) необхідно встановити діапазон частот, в якому має знаходитись приймальна частота. Після цього встановити необхідну частоту поворотом ручки вибору частоти (8).На межах діапазону поворот ручки (8) необхідно зупинити.

2 Порядок роботи з мікровольтметром.

2.1 Прослуховування модуляції.

Для прослуховування модуляції використовується гучномовець або навушники. Необхідна гучність встановлюється регулятором (10).

2.2 Порядок вимірювань

2.2.1 Калібрування приладу здійснити відповідно до п.1.1.

2.2.2 Приймальну частоту встановити відповідно до п. 1.2.

2.2.3 Перемикач режимів роботи (1) встановити в положення з позначкою Uп.

2.2.4 Регулятор затухання аттенюатора встановити таким чином, щоб покази стрілки індикатора прилада (2) знаходились в межах шкали. Тоді високочастотна вхідна напруга становитиме:

Ue(дБ)=D(дБ)+Ui(дБ),

де: *D(дБ)* - значення затухання аттенюатора;

Ui(дБ) - покази індикатора приладу.

3. Підготовка до роботи феромагнітної антени з активним підсилювачем

Феромагнітну антену зображено на рис. 1.2.

Для приведення її в робочий стан необхідно виконати наступні дії.

3.1 В корпус антени (1) вставити феромагнітні вставки (4), які відповідають вибраному діапазону частот. Позначення частотних діапазонів знаходиться на торцях(5) вставок. При під'єднанні феромагнітних вставок необхідно дотримуватись співпадання міток або на корпусі та на вставках.

3.2 Вимикач подачі живлення антенного підсилювача (7) поставити в положення «вимкн».

3.3 До гнізд антенного фідера та живлення антенного підсилювача, які знаходяться в торці корпусу (6) під'єднати відповідний філер.

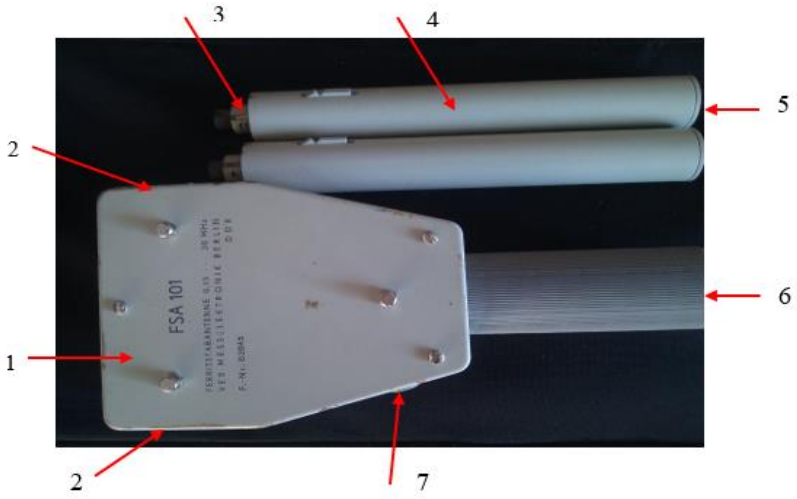

Рис. 1.2 Феромагнітна антена FSA-101

3.4 Протилежні кінці фідера під'єднати до гнізд (4) та (3) селективного мікровольтметра STV 301-2.

3.5 Вимикач живлення антенного підсилювача поставити в положення «увімкн.».

4. Запуск тестового сигналу.

4.1 На досліджуваному комп'ютері запустити програму TESTS1

4.2 Серед досліджуваних на предмет побічних електромагнітних випромінювань компонентів комп'ютера вибрати дослідження монітора.

4.3 Встановити вихідні параметри тестового сигналу відповідно до Табл. 1.1, де № варіанту відповідає № за списком студента в групі.

5. Вимірювання параметрів побічних електромагнітних випромінювань монітора комп'ютера.

5.1 На корпусі антени відімкнути подачу електроживлення на антенний підсилювач та вставити феромагнітні вставки з позначками «1».

5.2 Перемикач діапазонів частот селективного мікровольтметра STV 301-2 встановити в положення 1

5.3 Ручкою вибору частоти встановити мінімальну частоту діапазону.

Табл. 1.1

Параметри тестового сигналу

№ Вар.	Вид тесту	Частота мигання	Розмір				Отримана центр. частота
			a	b	c	d	
1	Клітки1	700	100	100	100	100	
2	Шахи	800	100	100	100	100	
3	Клітки2	900	100	100	100	100	
4	Клітки1	1000	150	150	150	150	
5	Шахи	700	150	150	150	150	
6	Клітки2	800	50	50	100	100	
7	Клітки1	900	100	100	50	50	
8	Шахи	1000	100	100	150	150	
9	Клітки2	800	150	100	100	150	
10	Шахи	900	180	180	180	180	
11	Клітки1	800	100	100	100	100	
12	Шахи	900	100	100	100	100	
13	Клітки2	1000	150	150	150	150	
14	Клітки1	700	150	150	150	150	
15	Шахи	800	50	50	100	100	

5.4 Увімкнути антенний підсилювач.

5.5 Зібрану феромагнітну антену встановити безпосередньо біля досліджуваного монітора комп’ютера.

5.6 Регулятор гучномовця встановити в середнє положення.

5.6 Плавно обертаючи ручкою вибору частоти в сторону збільшення частоти у вибраному діапазоні, на слух встановити наявність сигналу, модульованого тестовим сигналом монітора. В процесі пошуку модульованого тестового сигналу слідкувати за тим, щоб стрілка індикатора не виходила за межі шкали. Якщо стрілка наближається до межі шкали, необхідно змінити затухання вхідного сигналу регулятором атенюатора.

5.7 Зафіксувати першу найнижчу частоту, на якій виявлено модульований тестовий сигнал та абсолютну величину виміряної відповідно до п.2.2.4 напруги *Uе(дБ)*. Зазначені величини занести в табл. 1.2

Табл. 1.2

Показники вимірювання

№ комп'ю-тера	Відстань між антеною та монітором	*fmin* (МГц)	*Uе(дБ)*для *fmin*	Примітка

5.8 Не міняючи частоти вимірювання, встановити антену на відстані 15 см від монітора. Регулятором атенюатора встановити затухання вхідного сигналу таким, щоб стрілка індикатора знаходилась в межах шкали.

5.9 Здійснити вимірювання вхідного сигналу відповідно до п.2.2.4. Виміряну величину напруги занести в табл. 3 для частоти *f1*.

5.10 Збільшуючи частоту вимірювання, зафіксувати абсолютні величини виміряних напруг на частотах, де присутній модульований тестовий сигнал в діапазоні 1. Отримані дані занести в табл.3.

Табл.1.3

Амплітуди спектральних складових

Частота (МГц)	*f1*	*f2*	*f3*	*f4*		*fn*
Напруга (дБ)						

5.11 Здійснити вимірювання абсолютної напруги модульованого тестового сигналу в інших 5 діапазонах. Отримані дані занести в табл.3.

5.12 На підставі аналізу даних табл.1.3 побудувати векторну діаграму спектральної потужності побічних електромагнітних випромінювань(ПЕВ) монітора комп'ютера, відкладаючи по осі абсцис частоти гармонік, а по осі ординат – абсолютні виміряні напруги (рис 3).

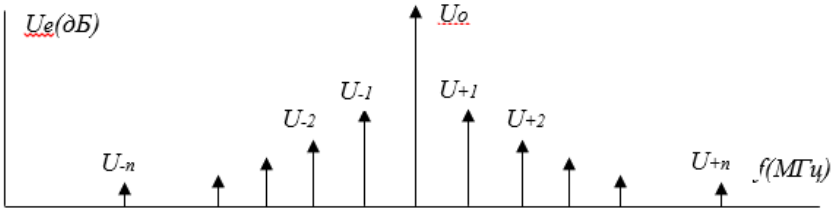

Рис. 1.3 Спектр основної та бокових гармонік сигналу ПЕВ *Ue(дБ)*

В звіті по лабораторній роботі подати:

1. Вихідні дані з табл. 1.1
2. Отримані дані (табл. 1.2)
3. Отримані дані (табл. 1.3)
4. Отриманий результат (Рис.1.3)

Лабораторна робота № 2
Створення просторового широкосмугового шумового сигналу для захисту комп'ютера від витоку інформації за рахунок побічних електромагнітних випромінювань

Мета роботи: Овоєння навиків застосування апаратури просторового електромагнітного зашумлення для локалізації небезпечних сигналів, які розповсюджуються через канали побічних електромагнітних випромінювань.

Завдання лабораторної роботи: визначити частоти основної та бічних гармонік побічних електромагнітних випромінювань. Дослідити порядок перекриття цих випромінювань за рахунок широкосмугового електомагнітного зашумлення.

Для виконання лабораторної роботи використовується вимірювальний комплект, який складається з селективного мікровольтметра STV 301-2, феритової стержневої антени FSA-101 та генератор радіошуму Ріас – 1М.

Органи управління та порядок роботи з приладом STV 301-2 та феритовою стержневою антеною FSA-101 описані в лабораторній роботі № 1.

Характеристиики приладу радіочастотного зашумлення «Ріас-1М»

Прилад призначений для створення електромагнітних завад в ефірі в діапазоні частот від 180 Гц до 2 ГГц. Коефіцієнт якості шуму - не менше ніж 0,8. Коефіцієнт міжспектральних кореляційних зв'язків - не менше ніж 2,0. Нормований рівень спектральної щільності напруги електричного і магнітного компонентів нормованого електромагнітного поля шуму - не менше ніж 30 дБ. Максимальна інтегральне значення вихідної потужності - не менше ніж 10 Вт.

Прилад створює маскуючий сигнал, що затруднює приймання і розкодування інформації, що міститься в електромагнітному випромінюванні, яке виникає при роботі різних електронних приладів і забезпечує:

- маскування побічних електромагнітних випромінювань засобів обчислювальної та офісної техніки;
- блокування радіоканалів, використовуваних пристроями дистанційного зняття інформації побічних електромагнітних випромінювань;
- блокування приймачів різних систем дистанційного керування по радіоканалу;
- блокування каналів витоку інформації через системи вторинної часофікації, радіофікації, телефонні системи, диспетчерські системи, системи охоронної та пожежної безпеки, системи енергопостачання та ін.

Прилад робить неможливим знімання інформації по побічних електромагнітних випромінюваннях від засобів обчислювальної та оргтехніки.

У зоні дії приладу може бути нестійким радіозв’язок (стільниковий, транкінговий пейджерний, побутовий радіотелефонний).

До складу приладу входять наступні пристрої:

- генератор радіочастотного шуму мобільний "РІАС-1ГМ" / 8 Вт;
- антени дипольні телескопічні "РІАС-1АД";

Прилад забезпечує формування стаціонарного випадкового сигналу з нульовим середнім значенням (білий шум) в діапазоні від 10 кГц до 2,5 ГГц потужністю не менше 8 Вт.

У приладі передбачена можливість регулювання потужності випромінювання на величину не менше 20 дБ.

Коефіцієнт якості шуму - не менше ніж 0,8.

Коефіцієнт міжспектральних кореляційних зв'язків - не менше ніж 2,0.

Максимальна інтегральне значення вихідної потужності - не менше ніж 5 Вт.

Спектральна щільність напруженості електричної і магнітної електромагнітного поля шуму відносно 1 мкВ на відстані 1 м від антени:

- в смузі частот від 10 кГц до 1000 МГц - не менше 60 дБ;
- в смузі частот від 1000 М Гц до 2000 МГц - не менше 50 дБ;
- в смузі частот від 2000 до 2500 МГц - не менше 40 дБ.

Прилад має вбудовану систему автоматичного контролю функціонування, звукову та світлову індикацію контролю функціонування.

Зовнішній вигляд приладу зображено на рис.2.1.

Рис.2.1 Прилад Ріас -1М

Порядок виконання лабораторної роботи

1. Для виконання лабораторної роботи необхідно налаштувати селективний мікровольтметр STV 301-2 на частоту основної гармоніки сигналу побічного електромагнітного випромінювання комп'ютера, визначену в ході виконання лабораторної роботи №1 (основна гармоніка повинна мати найвищу амплітуду спектра). Вставки феритової стержневої антени FSA-101 вибрати відповідно до діапазону, в якому знаходиться визначена частота.

2. На досліджуваному комп’ютері запустити програму TESTS1

2.1 Серед досліджуваних на предмет побічних електромагнітних випромінювань компонентів комп’ютера вибрати дослідження монітора.

2.2 Встановити вихідні параметри тестового сигналу відповідно до Табл. 2.1, де № варіанту відповідає № за списком студента в групі.

Табл. 2.1

Варіанти налаштування тестового сигналу

№ Вар.	Вид тесту	Частота мигання	Розмір				Отримана центр. частота
			a	b	c	d	
1	Клітки1	700	100	100	100	100	

2	Шахи	800	100	100	100	100	
3	Клітки2	900	100	100	100	100	
4	Клітки1	1000	150	150	150	150	
5	Шахи	700	150	150	150	150	
6	Клітки2	800	50	50	100	100	
7	Клітки1	900	100	100	50	50	
8	Шахи	1000	100	100	150	150	
9	Клітки2	800	150	100	100	150	
10	Шахи	900	180	180	180	180	
11	Клітки1	800	100	100	100	100	
12	Шахи	900	100	100	100	100	
13	Клітки2	1000	150	150	150	150	
14	Клітки1	700	150	150	150	150	
15	Шахи	800	50	50	100	100	

2.3 Підготувати до роботи прилад Ріас-1М, встановивши дипольні телескопічні антени взаємоперпендикулярно на максимальну робочу довжину. Встановити прилад Ріас-1М на столі, безпосередньо біля досліджуваного комп'ютера

2.4 Розташувати феритову стержневу антену FSA-101 безпосередньо біля монітора комп'ютера, здійснити вимірювання рівня побічних електромагнітних випромінювань на частоті основної гармоніки, покази індикаторного приладу селективного мікровольтметра STV 301-2 зафіксувати в табл.1., рядок *U*ПЕВ.

2.5 Не змінюючи частоти вимірювання STV 301-2, увімкнути прилад Ріас-1М, здійснити вимірювання рівня побічних електромагнітних випромінювань на частоті основної гармоніки з накладеним рівнем шумового сигналу, покази індикаторного приладу селективного мікровольтметра STV 301-2 зафіксувати в табл.1., рядок *U*Ш.

2.6 Розташовуючи антену FSA-101 через 1 м, повторити вимірювання, зазначені в п.п. 4, 5., на відстані 1-10 м. та зафіксувати їх в табл.2.2.

2.7 Побудувати в одній системі координат графік залежності рівнів побічних електромагнітних випромінювань та шумового сигналу

Табл. 2.2

Таблиця отриманих результатів

Відстань(м)	0	1	2	3	4	5	6	7	8	9	10
*U*ПЕВ (дБ)											
*U*Ш (дБ)											

В звіті по лабораторній роботі подати:

1. Вихідні дані з табл. 1
2. Отримані дані (табл. 1)
3. Отриманий результат у вигляді графіка.
4. Висновок щодо відстані, на якій рівень шумового сигналу перекриває рівень побічних електромагнітних випромінювань на частоті основної гармоніки

Лабораторна робота № 3
Дослідження політики облікових записів ОС WINDOWS XP

Мета роботи: Вивчити методи забезпечення безпеки робочої станції під керуванням ОС Windows. Навчитися налаштовувати рівні безпеки локального комп'ютера.

Ключові положення

Облікові записи користувачів дозволяють Microsoft Windows відслідковувати інформацію про користувачів і управляти їх правами доступу й привілеями. При створенні

облікових записів користувача, основними засобами керування обліковими записами є:

– Оснаска «*Користувачі й Комп'ютери Каталога Домена»* (*Active Directory Users And Computers), яка* використовується для керування обліковими записами користувачів у межі домена.

– Оснаска «*Локальні Користувачі й Групи»* (*Local User and Groups), яка* використовується для керування обліковими записами користувачів на локальному комп'ютері.

Облікові записи Windows використовують паролі й відкриті сертифікати, щоб засвідчувати доступ до ресурсів мережі. Пароль – це чутливий до регістра рядок, який містить до 104 символів у «*Службі каталога Active Directory»* і до 14 символів у «*Диспетчері безпеки Windows*». Щоб уникнути неавторизованого доступу до ресурсів мережі, потрібно використовувати безпечні паролі. Різниця між звичайним і безпечним паролем полягає у тому, що безпечний пароль важко вгадати й зламати. Важким для злому пароль робить комбінація всіх можливих типів символів, включаючи рядкові й заголовні літери, цифри й спеціальні символи.

Ключові питання

1. За допомогою яких інструментів можливе налаштування служб ОС Windows?

2. Поясніть, для чого служать відключені вами служби?

3.Поясніть призначення утиліти *msconfig*.

4. Для чого служить файл *boot.ini*?

5. Які налаштування безпеки ви можете зробити за допомогою утиліти «*Локальні політики*»?

6. За допомогою якого інструмента можливий доступ до редагування реєстру системи? Яким чином можна уникнути несанкціоновану або випадкову зміну реєстру користувачами системи?

7. За допомогою якого інструмента можна розмежувати права доступу до системного диска?

8. Яким чином можливе керування налаштування користувачів і груп? Які вимоги безпеки існують для настроювання користувачів і груп?

Завдання до лабораторної роботи

1. Вивчити засіб налаштування аутентифікації, реалізованої при вході вопераційну систему Windows. Для цього необхідно запустити утиліту «*Обліковізаписи користувачів*», набравши в командному рядку ім'я утиліти control userpasswords2 або з меню «*Мій комп'ютер/керування/локальні користувачі й групи*». Зробити зміни залежно від варіанта.

2. Налаштувати доступ користувачів і груп до файлів і директорій операційної системи Windows, для цього відкрити властивості директорії й вибрати вкладку «*Безпеки*» «*Security*». Зробити зміни, залежно від варіанта.

3. Налаштувати розмежування прав доступу користувачів і груп до ОС Windows за допомогою налаштування локальної політики, для цього запустити з командного рядка утиліту *secpol.msc*. Зробити зміни залежно від варіанта.

4. Налаштувати необхідні служби для роботи локального комп'ютера, відповідно до варіанта, для цього запустити утиліту *services.msc*. Перевірити список запущених служб, за допомогою виклику з командного рядка утиліти *cmd.exe* і команди *net start*.

5. Ознайомитися з налаштуваннями забезпечення безпеки ОС Windows, за допомогою оснащення «*Налаштування системи*», для цього запустити з командного рядка утиліту *msconfig*. Зробити зміни залежно від варіанта.

6. Налаштувати файл завантаження системи. Для цього необхідно, залежно від варіанта, зробити зміни параметрів завантаження у файлі *C:\boot.ini*.

7. Налаштувати рівні доступу в Інтернет стандартними способами ОС Windows *Internet Explorer* (низький, середній, високий). Зробити зміни, залежно від варіанта.

8. Налаштувати засоби автоматичного відновлення ОС Windows. Зробити зміни залежно від варіанта.

9. Налаштувати стандартний брандмауер ОС Windows (рівень захищеності – низький, середній, високий). Зробити зміни залежно від варіанта.

10. Забезпечити захист даних локальної робочої станції, за допомогою реєстру, для цього запустити утиліту *RegEdit* і зробити зміни залежно від варіанта

Варіанти завдань для виконання лабораторної роботи:

Варіант1.

1.1. Скасувати автоматичний вхід користувача в систему.

1.2. Створити директорію *temp* і налаштувати права доступу до даної директорії, таким чином, щоб користувачі, групи «*Гості*» мали права читання даних, огляду директорій, але не могли переглядати атрибути.

1.3. За допомогою однієї з доступних утиліт зупинити службу факсів, призначивши їй тип запуску: «*Вручну*».

1.4. У вікні «*Автозавантаження (startup)*», утиліти *msconfig* відключити автоматичний запуск всіх програм, крім антивірусу.

1.5. За допомогою *параметра /SOS включити* виведення на екран списку системних драйверів, які завантажуються під час початкового завантаження системи.

Варіант 2

2.1. Задати автоматичний вхід у систему, залишивши одного користувача.

2.2. Створити директорію *temp* і налаштувати права доступу до даної директорії таким чином, щоб користувачі, групи «*Оператори архіву*» не мали прав читання атрибутів, запису атрибутів, читання дозволів, зміну дозволів.

2.3. У вікні «*Служби (Services)*», утиліти *msconfig* відключити служби DHCP-*Клієнта*, координатора розподілених транзакцій, службу факсів.

2.4 Закрити доступ до запуску реєстру для всіх користувачів.

2.5. Скасуйте дію ключів */DEBUG*, для цього заборонити налагодження привілейованого режиму (ядра) під час ініціалізації, за допомогою параметра */NODEBUG.*

Варіант 3

3.1. Скасуйте вимогу натискання *Ctrl+Alt+Del* перед входом у систему.

3.2. Створіть директорію *temp* і налаштуйте права доступу до даної директорії таким чином, щоб користувачі, групи «*Досвідчені користувачі*» мали права читання, запису, видалення файлів, але не мали прав змінити дозволи і власника директорії.

3.3. Задайте функцію вимоги неповторності пароля, пароль повинен відповідати вимогам складності.

3.4. За допомогою однієї з доступних утиліт зупинити *службу завантаження зображень (WIA)*, призначивши тип запуску: «*Відключене*».

3.5. У вікні «*Файла завантаження (BOOT.INI)*», утиліти *msconfig* змінити час очікування входу в систему.

Варіант 4

4.1. Задайте обмеження терміну дії пароля користувача.

4.2. Створіть директорію *temp* і налаштуйте права доступу до даної директорії таким чином, щоб користувачі, групи «*Адміністратори*» мали повні права доступу.

4.3. Задайте максимальний термін дії пароля 14 днів, мінімальну довжину пароля 8 символів.

4.4. За допомогою однієї з доступних утиліт зупинити службу *COM запису компакт-дисків IMAPI*, призначивши їй тип запуску: «*Вручну*».

4.5. У вікні «*Автозавантаження (startup)*», утиліти msconfig відключити автоматичний запуск мультимедійних програм, таких як *Winamp, RealPlayer*.

Варіант 5

5.1. Дозвольте зміну пароля користувачем, додайте користувача в групу операторів налаштування мережі.

5.2. Створіть директорію *temp* і налаштуйте права доступу до даної директорії таким чином, щоб користувачі, групи «*Оператори налаштування мережі*» не мали прав видалення інформації і її редагування.

5.3. За допомогою параметра */PCILOCK,* скасуйте динамічний розподіл *IO/IRQ* для *PCI* пристроїв.

5.4. У вікні «*Служби (Services)*», утиліти *msconfig* відключіть служби диспетчера черги друку, старт-карт, *Telnet.*

5.5. Скасуйте використовувану за замовчуванням функцію ОС, що показує ім'я користувача, який останнім входив у систему, для цього у гілці реєстру *HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System* необхідно задати наступне значення параметра *DontDisplayLastUserName:DWORD = 1.*

Варіант 6

6.1. Перейменуйте обліковий запис адміністратора, задайте нестандартний шлях до профілю адміністратора.

6.2. Створіть директорію *temp* і налаштуйте права доступу до даної директорії таким чином, щоб користувачі, групи «*Користувачі вилученого робочого стола*» мали права переглядати, видаляти, створювати файли й директорії, але не могли змінити права доступу до них.

6.3. За допомогою однієї з доступних утиліт, зупиніть службу доступу до HID-*Пристроїв*, призначивши їй тип запуску: «Відключено».

6.4. За допомогою параметра */DEBUG* включіть налагодження

6.5. У вікні «*Файла завантаження* (*BOOT.INI*)», утиліти *msconfig* змінити завантаження ОС у захищеному режимі з підтримкою мережі, за допомогою параметра *SAFEBOOT* і додаткового ключа *NETWORK*.

Варіант 7

7.1. Налаштуйте вимогу до зміни пароля користувача, при наступному вході в систему, підключіть користувача до мережного профілю. 7

7.2. Створіть директорію «*temp*» і змініть власника даної директорії.

7.3. За допомогою параметра */NUMPROC=*, визначте число процесорів, які будуть використовуватися в мультипроцесорній системі.

7.4. За допомогою однієї з доступних утиліт зупиніть службу диспетчера сеансу довідки для вилученого робочого столу, призначивши їй тип запуску: «*Вручну*».

7.5. У вікні «*Автозавантаження (startup)*», утиліти *msconfig* відключити автоматичний запуск офісних програм, наприклад *Microsoft Office TSR*.

Варіант 8

8.1. Перейменуйте обліковий запис гостя. Створіть нового користувача, додайте його в групу операторів архіву.

8.2. Створіть директорію «*temp*», закрийте директорію від всіх
користувачів, крім групи адміністраторів.

8.3. Налаштуйте аудит відстеження процесів.

8.4. У вікні «*Служби (Services)*», утиліти *msconfig* відключити служби джерела безперебійного живлення, службу підтримки *TCP/IP NetBIOS*

8.5. За допомогою параметра */BASEVIDEO* налаштуйте використання стандартного *VGA* драйвера в графічному режимі.

Варіант 9

9.1. Обмежте використовуваний ОС Windows обсяг пам'яті, указавши параметр *MAXMEM=16*.

9.2. Налаштуйте права доступу до локального диска *D:*\\ і застосуйте спадкування даних прав до піддиректорій.

9.3. Налаштуйте аудит успішного й невдалого доступу до служби каталогів.

9.4. За допомогою однієї з доступних утиліт запустіть службу журналів і оповіщення продуктивності, призначивши їй тип запуску: «*Авто*».

9.5. У вікні «*файла завантаження (BOOT.INI)*», утиліти *msconfig* вкажіть, за допомогою параметра *ALTERNATESHELL*, яку

графічну оболонку використовувати за замовчуванням, замість *Explorer'a.*

Варіант 10

10.1. Включіть налагодження й установіть швидкість передачі даних, замість передбаченої за замовчуванням (19200), за допомогою параметра */BAUDRATE=115200*.

10.2. Перегляньте діючі дозволи користувачів, що входять у групу *«Users»* на диск *D:*\\

10.3. Налаштуйте аудит успішних і невдалих входів користувачів у систему.

10.4. За допомогою однієї з доступних утиліт запустіть службу тіньового копіювання тома, призначивши їй тип запуску: «*Авто*».

10.5. У вікні «*Автозавантаження (startup)*», утиліти *msconfig* відключити автоматичний запуск систем керування базами даних, таких як *Microsoft SQL Server*.

Варіант 11

11.1. Налаштуйте доступ до вилученого редагування реєстру для групи адміністраторів домена.

11.2. Створіть директорію «*temp*», налаштуйте права доступу до даної директорії групі «*Users*», задавши право читання, перегляду й запуску файлів, тільки в даній директорії.

11.3. Налаштуйте заборону входу в систему через службу терміналів.

11.4. У вікні «*Служби (Services)*», утиліти *msconfig* відключити служби планувальника завдань.

11.5. За допомогою параметра */ONECPU* укажіть використання одного процесора.

Варіант 12

12.1. Налаштуйте щомісячну зміну паролів.

12.2. За допомогою параметра *SAFEBOOT* і додаткового ключа *MINIMAL* задайте завантаження ОС Windows у захищеному режимі без підтримки мережі.

12.3. Налаштуйте право на завершення роботи системи, тільки для групи «*Адміністратори*».

12.4. За допомогою однієї з доступних утиліт, запустіть службу центра забезпечення безпеки, призначивши їй тип запуску: «*Авто*».

12.5. У вікні «*Файла завантаження (BOOT.INI)*», утиліти *msconfig* змінити час очікування входу в систему.

Звіт про виконану роботу

1. Назва роботи.
2. Мета роботи.
3. Пункти виконаного завдання.
4. У звіті про виконання лабораторної роботи, необхідно включити змінені параметри, інструмент (утиліти, команди), за допомогою яких вироблялися зміни, опис призначення кожного зміненого параметра й зроблених вами налаштувань.
5. Висновки

Лабораторна робота № 4
Ознайомлення з інструкцією системного адміністратора комплексу засобів захисту «Гриф-ХР».

Мета роботи: ознайомитись з інструкцією системного адміністратора КЗЗ «Гриф ХР» для подальшого використання його положень при виконанні першого етапу інсталяції на робочу станцію комплексу.

Завдання лабораторної роботи: ознайомитись з вимогами інструкції системного адміністратора комплексу засобів захисту від несанкціонованого доступу, розміщеною в якості додатка до лабораторної роботи № 4 навчальної дисципліни «Основи теорії захисту інформації» в навчальній платформі Moodle за посиланням: http://exam.nuwm.edu.ua/pluginfile.php/97261/mod_resource/content/1/gxp_103i.pdf.

Підготувати відповіді на наступні питання:

1. Що входить до обов'язків системного адміністратора КЗЗ «Гриф»?
2. Які попередні дії необхідно реалізувати перед інсталяцією комплексу на АС?
3. Який порядок інсталяції комплекса на АС?
4. Які операції виконує програма інсталяції на першому етапі?
5. Опишіть порядок першого завантаження ОС та вводу ліцензії.
6. Назвіть початкові налаштування системи.
7. Опишіть порядок створення облікових записів адміністраторів.
8. Опишіть порядок відключення непотрібних служб ОС.
9. Опишіть порядок перевірки цілісності ПЗ КЗЗ «Гриф».
10. Оришіть порядок деінсталяції комплекса КЗЗ «Гриф».

Лабораторна робота № 5
Інсталяція комплексу засобів захисту «Гриф-ХР»

Мета роботи: освоїти порядок першого етапу інсталяції на робочу станцію комплексу засобів захисту (КЗЗ) «Гриф ХР».

Ключові положення

Засоби та комплектуючі для виконання лабораторної роботи:

1. Робоча станція (автоматизована система класу 1) під управлінням ОС Windows-XP, не підключена до локальної та глобальної мереж.

2. Завантажувальний диск «Комплекс засобів захисту інформації від несанкціонованого доступу Гриф- ХР»

Виконання лабораторної роботи розділено на 2 частини:

1 частина – перевірка та підготовка BIOS робочої станції;

2 частина – виконання першого етапу інсталяції КЗЗ «Гриф- ХР».

3

Завдання лабораторної роботи: Виконати перший етап інсталяції КЗЗ Гриф-ХР згідно нижченаведеної методики.

5.1. Перевірка та підготовка BIOS робочої станції

Зайти в BIOS робочої станції: жорсткий диск (IDE або SATA), на якому встановлена ОС, повинен бути підключений як провідний диск на головному каналі контролера (Primary Master);

Для того, щоб SATA диск було видно як Primary Master, рекомендується встановити в Setup BIOS наступні настройки контролера IDE (на тих BIOS, де вони підтримуються):

Onboard IDE Operation Mode = Enhanced Mode
Enhanced Mode Support On = P-ATA

завантажувальний розділ жорсткого диска повинен бути першим розділом на першому жорсткому диску;

· На ПЕОМ повинна бути встановлена тільки одна ОС - Windows XP (з пакетом оновлення не вище SP2);

· На ПЕОМ повинна бути встановлені тільки стандартні засоби завантаження ОС(повинні бути відсутні засоби, які підтримують багатоваріантну систему завантаження MultiBoot);

· Для контролю послідовності завантаження використовується емпіричний алгоритм - існує ймовірність, що для певних BIOS зміна довільних налаштувань Setup може бути сприйнята як зміна послідовності завантаження.

Незалежно від того, чи використовуються апаратна частина КЗЗ, для експлуатації «Гриф-XP» необхідно виконання наступних обмежень:

· ОС повинна бути встановлена в каталозі, що знаходиться в корені логічного диска (Наприклад, C: \ WINDOWS);

· Робоча станція Windows XP, на яку проводиться установка, не повинна бути членом домену і довжина імені робочої станції не повинна перевищувати 14 символів (Див. Діалог «Система | Властивості | Мережева ідентифікація»);

Перед установкою КЗЗ від несанкціонованого доступу "Гриф-XP» необхідно:

· Перевірити і забезпечити виконання наведених вище умов;

· перевірити ПЕОМ на відсутність вірусів;

· Конвертувати всі FAT і FAT32 розділи жорстких дисків в NTFS наприклад, використовуючи утиліту ОС Convert);

· Відключити антивірусні засоби, що функціонують в режимі безперервного

моніторингу, до повного завершення установки комплексу.

5.2. Інсталяція початкових налаштувань КЗЗ «Гриф- XP».

Для установки КЗЗ від несанкціонованого доступу "Гриф-XP» необхідно:

· Перейменувати обліковий запис "Адміністратор" в англомовний, наприклад "Admin". Користувач, що відповідає даній облікового запису буде виступати в ролі системного адміністратора (СА). Після перейменування облікового запису необхідно перевантажити ПЕОМ або завершити поточний сеанс роботи.

· Встановити пароль на доступ до Setup BIOS. Довжина пароля повинна бути не менше восьми символів (якщо максимально дозволена довжина пароля менш восьми символів, то слід задавати пароль максимально можливої довжини);

· Ввійти до системи з обліковим записом системного адміністратора.

· Створити каталог еталонної копії ПО КЗЗ. Ім'я каталогу може бути будь-яким крім C: \ G2K і C: \ G2Kinst (наприклад, D: \ G2KEtalon).

· Вставити інсталяційний диск в дисковод. Перед установкою КЗЗ прочитайте файл _readme, який знаходиться на диску, - він може містити свіжі відомості, які не увійшли до даної інструкції. Крім того, зверніть увагу на каталоги Patch_xx, які можуть бути присутніми на диску і містять оновлення ПЗ КЗЗ. Зокрема, в них може міститися оновлена редакція самої програми інсталяції.

· Запустити програму GXPLocal.exe, яка знаходиться на інсталяційному диску КЗЗ.

· Встановлення системи виконується в два етапи і може бути перервана в будь-який момент натисканням кнопки [Скасувати]

Якщо в процесі установки КЗЗ робота програми інсталяції з якої-небудь причини була перервана, процес установки можна відновити з початку поточного кроку інсталяції, запустивши програму setup.exe з каталогу C: \ G2KInst. Повідомлення про помилки наведені в розділі "Налаштування від помилок". У випадку необхідності відкату, не виконуйте його "вручну". Відкат (деінсталяцію) можна виконати, запустивши програму setup.exe з каталогу C: \ G2K з ключем / Uninstall.

На першому етапі програма установки виконує наступні операції:

- копіює необхідні для установки КСЗ файли на жорсткий диск ПК (в каталог C: \ G2KInst) і вся подальша установка проводиться з цього каталогу;

- видає запит про необхідність використання апаратного захисту від несанкціонованої завантаження: «Чи будете Ви використовувати плату з ПЗУ КСЗ "Гриф-ХР" для захисту ПК від несанкціонованого завантаження?» (Рис4.1);

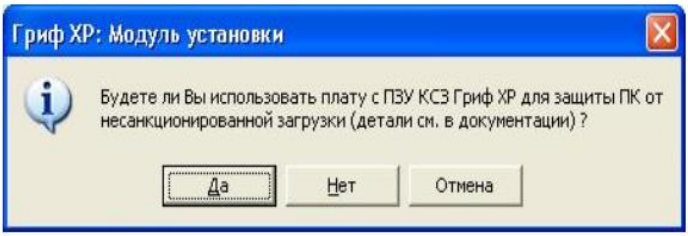

Рис. 4.1

Слід зазначити, що перемикання між конфігураціями не допускається. Якщо на даний запит Ви відповісте негативно - апаратний захист не зможе бути використано в подальшому без перевстановлення КЗЗ. Якщо позитивно – звичайні користувачі не зможуть входити в ОС при відсутності плати з ПЗУ КСЗ.

Якщо на інсталяційному диску міститься оновлена редакція програми інсталяції (setup.exe), рекомендується використовувати її. Для цього слід перервати інсталяцію на даному етапі (натиснути кнопку [Скасувати]), переписати з інсталяційного диска оновлену програму інсталяції (setup.exe) в каталог C: \ G2Kinst поверх існуючої і запустити її.

Після вибору конфігурації КЗЗ програма установки:

- виводить нагадування про необхідність установки послідовності завантаження «A :, C:», якщо обрана конфігурація з використанням апаратних засобів (рис.4.2);

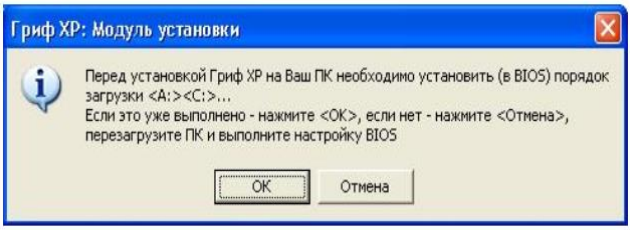

Рис. 4.2

- виводить вікно з привітанням, а потім - ліцензійну угоду і вимагаєпідтвердити згоду з його положеннями;

- просить вибрати створений раніше каталог для збереження еталонної копії ПЗ (Рис.4.3);

В якості каталогу еталонної копії ПЗ можна вибрати будь-який каталог (включаючи каталоги на змінних носіях) крім C: \ G2K, C: \ G2Kinst і каталогу ОС (якщо вибраний каталог знаходиться на диску з файловою системою NTFS, то згодом для обмеження доступу до нього адміністратор КСЗ може встановити на даний каталог захист з рівнем «Технологічна програма» і надати до нього доступ тільки адміністраторам).

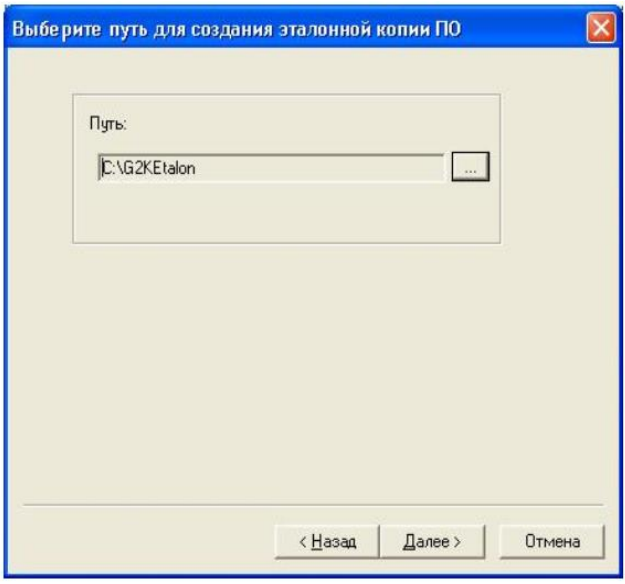

Рис. 4.3

Після того, як адміністратор вибрав каталог еталонної копії і підтвердив готовність продовжити установку, програма:

- перевіряє відповідність конфігурації ПЕОМ необхідній;
- копіює необхідні для роботи КСЗ файли на жорсткий диск ПЕОМ в каталог «С: \ G2K» (каталог КЗЗ має фіксоване ім'я і його перейменування або зміна структури підкаталогів не допускається) (рис. 4.4);

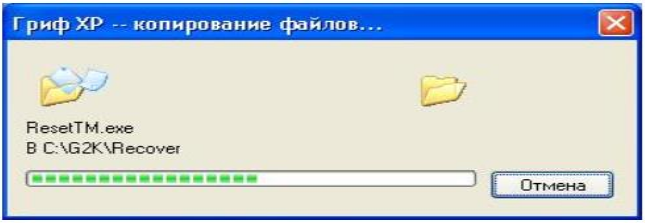

Рис. 4.4

- перевіряє наявність необхідних повноважень у поточного користувача;

- виконує настройку привілеїв користувачів відповідно до реалізованої КЗЗ політики безпеки (ПБ);

- видаляє всі групи користувачів, крім вбудованих;

- видаляє всі облікові записи користувачів, крім облікового запису системного адміністратора ("Admin") і "Гість" (при цьому обліковий запис "Гість" відключається);

- створює службові групи користувачів КСЗ «Гриф-ХР», додає в нихсистемного адміністратора ("Admin").

Після цього інсталятор повідомить про необхідність установки

послідовності завантаження «C :, ...» (рис. 4.5) і при виході ініціює перезавантаження ПЕОМ.

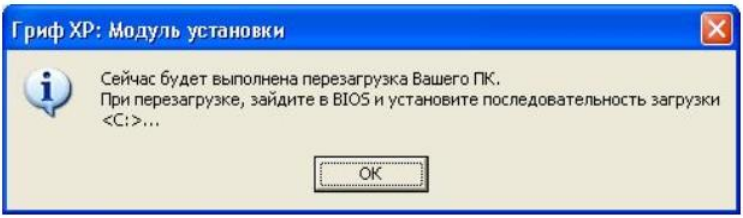

Рис. 4.5

Якщо обрана конфігурація з використанням апаратних засобів, то в процесі перезавантаження обов'язково необхідно увійти в Setup BIOS і встановити еталонну послідовність завантаження. Якщо в Setup BIOS пріоритетність завантаження задається шляхом вибору зі списку, встановити послідовність завантаження «C: only» або «C:, A:». Якщо в Setup BIOS пріоритетність завантаження задається шляхом вказівки 1-го, 2-го, 3-го і т.д. завантажувального пристрою, встановити таку послідовність завантаження: перший завантажувальний пристрій - HDD, друге - FDD (Floppy), третє - LAN;

Для продовження процесу установки необхідно заново увійти в ОС під обліковим записом системного адміністратора ("Admin"). Після успішного входу в ОС розпочнеться другий етап установки КЗЗ «Гриф-ХР».

На цьому процес інсталяції КЗЗ «Гриф-ХР зупиняється, умови вимог лабораторної роботи вважаються виконаними.

Необхідно здійснити деінсталяцію запустивши програму setup.exe з каталогу C: \ G2K з ключем / Uninstall.

Лабораторна робота № 6
Вивчення функціональних характеристик комплексу засобів захисту «Лоза-1»

Мета: вивчити основні функціональні можливості КЗЗ «Лоза-1»

Завдання лабораторної роботи: ознайомитись з основними функціональними характеристиками програмного комплексу засобів захисту «Лоза», розміщеними за посиланням: «Загальний опис системи» http://avtoprom.kiev.ua/PDF/LOZA-1_SecDescr.pdf

Користуючись вищенаведеним ресурсом, підготувати письмові відповіді на 6 питань, зазначених в табл. 6.1.

Табл. 6.1

Варіанти вибору з переліку питань

№ за списком в групі	№№ питань
1	1, 15, 21, 43, 48, 55
2	4, 19, 25, 37, 46, 54
3	8, 13, 23, 29, 51, 55,
4	12, 22, 27, 33, 41, 55
5	4, 16, 22, 31, 37, 49
6	8, 17, 20, 36, 41, 43
7	7, 12, 19, 24, 40, 45
8	6, 16, 19, 28, 44, 49
9	5, 18, 29, 32, 50, 54
10	3, 11, 23, 36, 41, 54,
11	6, 13, 27, 35, 40, 55,
12	7, 11, 19, 25, 31, 44
13	8, 14, 15, 32, 35, 48,
14	9, 18, 29, 38, 47, 52,
15	2, 11, 22, 43, 48, 53
16	5, 14, 26, 37, 46, 55

17	9, 19, 30, 36, 44, 51
18	5, 13, 17, 34, 38, 44
19	6, 11, 17, 22, 38, 41,
20	4, 18, 21, 33, 38, 50

Перелік питань загального опису системи «Лоза-1»

1. Під керуванням яких операційних систем може працювати система ЛОЗА-1?
2. Яке основне призначення КЗЗ Лоза-1?
3. Які операції можуть виконуватись під час роботи системи?
4. Який порядок роботи системи після виявлення помилки?
5. Які можливі варіанти продовження роботи видає програма «Монітор захисту» після виявлення помилки?
6. Яких значень може набувати режим роботи системи?
7. Які відомості містяться в облікових записах користувачів програми «Керування захистом»?
8. Які ролі користувачів визначені для розподілу обов'язків у системі?
9. Які рівні допуску користувачів визначені системою.
10. Для чого призначені ключові диски в системі?
11. З яких параметрів конфігурації складається політика паролів?
12. Виконання яких вимог забезпечують необхідну складність пароля?
13. Які правила визначено політикою блокування облікових записів?
14. Якими параметрами визначається порядок входу користувачів до системи?
15. В яких об'єктах система ЛОЗА-1 дозволяє захистити інформацію?
16. Яких значень можеже набувати принцип керування доступом атрибутів баз документів?
17. З якого переліку обираєтьс я максимальний рівень доступу документів атрибутів баз документів?

18. З якого переліку обираєтьс я мінімальний рівень доступу документів атрибутів баз документів?
19. Що означає обмеження для адміністратора документів, визначене політикою документів?
20. Що означає примусове маркування документів перед друком, визначене політикою документів?
21. Які атрибути документа входять до переліку стандартних?
22. Назвіть атрибути доступу документа і їхні початкові значення.
23. Що означають базові види доступу до документів?
24. Назвіть атрибути захищених папок і вказані їхні початкові значення.
25. Які види доступу встановлюються для знімних дисків?
26. Назвіть атрибути зареєстрованого диска USB Flash.
27. Які модуль операційної можуть належати до списку захищених процесів?
28. Які дані належать до технологічної інформації?
29. До яких об'єктів застосовується довірче керування доступом?
30. До яких об'єктів застосовується адміністративне керування доступом?
31. При виконанні яких умов користувач отримує доступ до баз документів?
32. Які види доступу до баз документів отримує її власник, якщо він є звичайним користувачем?
33. Які види доступу до баз документів не можуть отримати звичайні користувачі?
34. Якщо користувачу встановлена роль Звичайний користувач, він є власником документа і його рівень допуску не нижчий за рівень доступу документа, то які види доступу він отримує до документа?
35. За яких умов користувач отримує доступ до зареєстрованого диска USB Flash?
36. За яких умов користувач отримує доступ до захищених процесів?

37. Які команди програм Microsoft Excel та Microsoft Word називаються небезпечними?
38. Які параметри конфігурації використовуються для встановлення заборонених програм?
39. Які вимоги відстежує система ЛОЗА-1 для забезпечення обмежень на роботу користувачів?
40. Які об’єкти захисту можуть бути безпечно видалені за допомогою системи Лоза-1?
41. Які параметри конфігурації передбачені для автоматичного видалення тимчасових файлів?
42. Які механізми захисту використовуються для контролю друку документів?
43. Які параметри конфігурації встановлюються для заборони друку документів?
44. Цілісність яких об’єктів може бути перевірена за допомогою параметра конфігурації «об’єкти для перевірки цілісності»?
45. Якими параметрами конфігурації визначається перелік файлів та папок, які перевіряються на цілісність?
46. Які порушення цілісності можуть бути виявлені в результаті перевірки?
47. Якими параметрами конфігурації визначається перелік розділів та параметрів реєстру, які перевіряються на цілісність?
48. Які порушення цілісності можуть бути виявлені при перевірці завантажувальних секторів?
49. За допомогою якого методу обчислюються контрольні суми для відстеження змін об’єктів?
50. Які події реєструються в журналі дій користувачів?
51. Які функції виконує журнал реєстрації?
52. Які параметри конфігурації має перелік небезпечних подій?
53. Яка інформація зазначається в протоколі друку програми «Аудитор»?
54. Які події належать до джерела LOZAAudit?
55. Де зберігаються файли звітів про небезпечні події?

Лабораторна робота № 7
Встановлення параметрів входу до системи. Встановлення параметрів захисту друку та експорту документів

Мета роботи: набуття досвіду конфігурації комплексу засобів захисту при налаштуванні параметрів входу до системи та встановлення параметрів захисту друку та експорту документів.

Завдання лабораторної роботи

На автоматизованій системі класу 1, де встановлено комплекс засобів захисту «Лоза-1», ввійти під обліковим записом «Адміністратор безпеки» та здійснити налаштування згідно нижчезаначеної методики.

7.1. Встановлення параметрів входу до системи

Вхід до системи регулюється такими параметрами конфігурації системи:

- дозволяти вхід до Windows тільки користувачам системи;
- перевіряти ключовий диск під час входу до Windows;
- перевіряти ключовий диск під час роботи у Windows;
- відображати ім'я попереднього користувача;
- дозволяти вхід до Windows тільки в робочому стані системи.

Усі наведені параметри можуть приймати значення *Так* та *Ні*.Якщо параметр конфігурації Дозволяти вхід до Windows тільки користувачам системи має значення *Так*, це матиме такі наслідки: увійти до Windows зможуть тільки користувачі, які мають обліковий запис у системі ЛОЗА-1;

- замість стандартних діалогів входу до Windows, виходу з Windows (викликається натисканням комбінації клавіш *Ctrl+Alt+Del* після успішного входу до системи), розблокування комп'ютера та зміни пароля використовуватимуться відповідні діалоги системи ЛОЗА-1;

- під час входу до системи користувачі будуть змушені використовувати комбінацію клавіш *Ctrl+Alt+Del*;

- буде відключена можливість запуску програм від імені іншого користувача;

- будуть відключені екран привітання Windows XP та можливість швидкого переключення між користувачами Windows XP. Значення параметрів відображати ім'я попереднього користувача, дозволяти вхід до Windows тільки в робочому стані системи та перевіряти ключовий диск під час входу до Windows можна встановлювати тільки в тому випадку, коли для параметра дозволяти вхід до Windows тільки користувачам системи встановлене значення *Так*.

Значення Так параметра конфігурації перевіряти ключовий диск під час входу до Windows означає, що увійти до системи та розблокувати комп'ютер можуть тільки ті користувачі, які мають обліковий запис у системі ЛОЗА-1 та за необхідності ключовий диск.

Значення *Так* параметра конфігурації *перевіряти ключовий диск під час роботи у Windows* означає, що у випадку видалення ключового диска під час роботи комп'ютер автоматично блокується. Значення цього параметра можна встановлювати тільки в тому випадку, коли для параметра перевіряти ключовий диск під час входу до Windows встановлене значення *Так*.

Значення *Так* параметра конфігурації *відображати ім'я попереднього користувача* означає, що в діалозі входу до системи буде відображатись ім'я попереднього користувача.

Значення *Так* параметра конфігурації *дозволяти вхід до Windows* тільки в робочому стані системи означає, що звичайні користувачі та адміністратори документів можуть увійти до Windows тільки під час перебування системи в робочому стані.

7.2 Встановлення параметрів захисту друку та експорту документів

Система надає можливості для захисту документів під час їх друку та експорту (збереження у файлі). Ці можливості рекомендується використовувати при роботі із секретною інформацією.

Захист друку документів регулюється за допомогою таких параметрів конфігурації:

- захищати друк документів паролем;

- пароль на друк документів.

Надання параметру конфігурації захищати друк документів паролем значення Так означає, що користувач отримуватиме доступ на друк документа лише за умови введення паролю на друк, що забезпечує присутність під час друку уповноваженої особи.

Для встановлення пароля адміністратор за допомогою програми *Керування захистом* викликає відповідне вікно та запрошує уповноважену особу ввести пароль.

Обмеження для пароля (мінімальна довжина, складність, термін дії і т. ін.) не передбачаються, – уповноважена особа, що використовує пароль, встановлює відповідні правила на власний розсуд.

Захист експорту документів здійснюється аналогічним чином. Для цього використовуються такі параметри конфігурації:

- захищати експорт документів паролем;
- пароль на експорт документів.

наведені параметри можуть приймати значення *Так* та *Ні*

Лабораторна робота № 8
Встановлення параметрів ключових дисків. Блокування дисків

Мета роботи: отримання досвіду конфігурації комплексу засобів захисту при налаштуванні параметрівключовихх дисків та блокування дисків.

Завдання лабораторної роботи

На автоматизованій системі класу 1, де встановлено комплекс засобів захисту «Лоза-1», ввійти під обліковим записом «Адміністратор безпеки» та здійснити налаштування згідно нижчезаначеної методики.

8.1 Встановлення параметрів ключових дисків

Система надає можливість використовувати для автентифікації користувача не тільки пароль, а й фізичні ідентифікатори – ключові диски, що значно підвищує надійність автентифікації.

Як ключові диски можуть використовуватись дискети та/або модулі пам'яті USB-Flash із файловою системою FAT.

Використання ключових дисків регулюється такими параметрами конфігурації системи:

- гнучкі ключові диски;
- знімні ключові диски.

Ці параметри встановлюють, які саме диски будуть використовуватись для автентифікації користувача. Для автентифікації можуть використовуватись всі гнучкі та/або знімні диски або вибрані.

8.2 Диски для зберігання документів

Система ЛОЗА-1 дозволяє зберігати бази документів на жорсткому диску та на знімних носіях – дискетах, модулях пам'яті USB Flash, компакт-дисках (без можливості запису), Zip-дисках тощо.

Для того щоб адміністратор безпеки мав змогу вказати, де саме повинні зберігатись бази документів, використовуються такі параметри конфігурації:

- гнучкі диски для зберігання документів;
- компакт-диски для зберігання документів;
- знімні диски для зберігання документів;
- жорсткі диски для зберігання документів.

Всі параметри можуть приймати значення *Всі диски* або містити фіксований перелік букв, які відповідають дискам певного типа (наприклад, *F:, G*:).

Документи зберігаються в кореневій папці зазначеного диска в папці *LOZADoc*.

Зберігати документи на жорстких дисках (тобто на розділах жорсткого диска) можна лише в тому випадку, коли вони використовують файлову систему NTFS. Для папки LOZADoc на фіксованому диску встановлюються ті ж дозволи на доступ, що і для папки *%LOZA%\Doc*. Це унеможливлює доступ до папки для всіх користувачів системи. Незмінність встановлених дозволів перевіряється під час перевірки цілісності файлів та папок.

Для унеможливлення доступу користувачів до документів, які зберігаються на гнучких дисках, компакт-дисках та знімних дисках, рекомендується блокувати ці диски.

8.3 Блокування дисків

Блокування дисків використовується для унеможливлення безпосереднього доступу звичайних користувачів до даних, які зберігаються на знімних носіях.

Звичайні користувачі та адміністратори документів безпосереднього доступу до заблокованого диска не мають. Вони можуть отримати доступ до даних лише за допомогою програми Захищені документи. Адміністратори безпеки та системні адміністратори мають до заблокованого диска повний доступ.

Заблокувати можна будь-яку кількість знімних дисків. Диски блокуються на весь час роботи системи, незалежно від стану, у якому вона перебуває. Перелік знімних дисків, які блокуються, визначається такими параметрами конфігурації:

- блокування гнучких дисків;
- блокування знімних дисків;
- блокування компакт-дисків.

Параметри блокувати знімні диски та блокувати компакт-диски

можуть приймати лише два значення: *всі диски* та *всі диски з документами*. Значення *всі диски з документами* означає, що блокуватись будуть лише ті диски, на яких зберігаються бази документів.

Для параметра *блокувати гнучкі диски* можуть бути вказані значення неблокувати та всі диски або явно вказані диски, які слід блокувати (наприклад, диск А:).

Ці параметри дозволяють виконати одночасно два описані нижче завдання.

1) Заблокувати всі диски, на яких зберігаються бази документів. Блокування цих дисків є необхідною умовою використання системи ЛОЗА-1 в. п. 2.5.2.

Знімні диски та компакт-диски, на яких зберігаються бази документів, будуть заблоковані автоматично, а для гнучких дисків блокування повинен встановити адміністратор.

2) Заблокувати взагалі всі знімні диски або всі знімні диски певного типу на комп'ютері. Це може бути необхідно, наприклад, для унеможливлення неконтрольованого використання знімних дисків.

Лабораторна робота № 9
Підготовка Встановлення параметрів заборони друку. Встановлення політики аудита

Мета роботи: отримання досвіду конфігурації комплексу засобів захисту при налаштуванні параметрів заборони друку та встановлення політики аудита.

Завдання лабораторної роботи

На автоматизованій системі класу 1, де встановлено комплекс засобів захисту «Лоза-1», ввійти під обліковим записом «Адміністратор безпеки» та здійснити налаштування згідно нижчезаначеної методики.

9.1 Встановлення параметрів заборони друку

Система ЛОЗА-1 надає можливість повністю контролювати друк документів, які обробляються за допомогою програми Захищені документи. Для цього можуть бути використані такі механізми:

- встановлення дозволу/заборони друку документа;
- встановлення аудиту друку документа, що забезпечує докладну реєстрацію
- подій друку;
- встановлення пароля на друк.

Під час роботи за допомогою інших програмних засобів перелічені механізми не можуть бути задіяні. Для таких випадків у системі передбачена можливість повної або часткової заборони друку, а також можливість тимчасового дозволу друку.

Для встановлення заборони друку використовуються два параметри конфігурації:

- спосіб заборони друку;
- облікові записи для заборони друку.

Перший параметр визначає, кому саме заборонений друк, і може приймати такі значення:

- нікому (друк дозволений всім);
- всім (друк заборонений всім);
- всім користувачам системи ЛОЗА-1, крім адміністраторів
- безпеки;
- всім користувачам системи ЛОЗА-1, крім адміністраторів
- документів;
- всім користувачам системи ЛОЗА-1, крім адміністраторів
- безпеки та документів;
- спеціальна настройка.

Якщо параметр спосіб заборони друку має значення спеціальна настройка, друк забороняється для облікових записів, які перелічені в параметрі облікові записи для заборони друку.

Заборона друку, яка визначається зазначеними параметрами, встановлюється на початку роботи системи та під час кожного входу користувача до системи (якщо для параметра дозволяти вхід до Windows тільки користувачам системи має значення *Так*).

Для того, щоб тимчасово дозволити користувачу друк, не вимагаючи його виходу із системи, адміністратор може скористатись утилітою Помічник адміністратора, яка заходить у папці %LOZA%\Lib (файл AdminAssistant.exe).

Після запуску утиліти адміністратор повинен вказати своє ім’я, пароль та ключовий диск (останнє – якщо параметра перевіряти ключовий диск під час входу до Windows має значення *Так*). Утиліта надає можливість тимчасово дозволити друк. Адміністратор вказує також «термін дії» тимчасового дозволу на друк, обираючи один з двох варіантів:

- *до заборони друку адміністратором* – це означає, що для відновлення заборони друку адміністратор повинен знову скористатись утилітою Помічник адміністратора;

- *поки встановлений ключовий диск адміністратора* (цей варіант доступний лише тоді, коли параметр перевіряти ключовий диск під час входу до Windows має значення Так).

9.2 Встановлення політики аудита

Політика аудита визначається однойменним параметром конфігурації системи (параметр політика аудита) і визначає, які саме дії користувачів можуть бути зареєстровані в журналі захисту. Політика аудита встановлюється окремо для таких категорій:

- вхід/вихід (вхід користувачів до системи ЛОЗА-1, зміна пароля користувача, вихід із системи та ін.);
- робота з програмами (запуск та завершення роботи прикладних програм системи);
- керування доступом (коригування бази даних захисту);
- керування системою (зміна стану системи, визначення початкового стану для наступного сеансу роботи та ін.);
- конфігурація (читання та зміна значень параметрів конфігурації);
- доступ до документів (читання, коригування, друк документів, коригування атрибутів доступу документів та ін.);
- доступ до баз документів.

Встановлення аудита для всіх категорій, крім двох останніх, призводить безпосередньо до реєстрації відповідних подій у журналі.

Встановлення аудита подій доступу до документів та баз документів лише дозволяє реєстрацію відповідних подій. Для того щоб вони були зареєстровані, необхідно щоб аудит був також встановлений у списку аудита відповідного об’єкта.

Політика аудита може бути встановлена досить гранульовано. Для параметрів конфігурації аудит може бути встановлений окремо для різних груп параметрів. Для подій доступу до документів аудит може бути встановлений у залежності від рівня доступу документа, а для подій доступу до баз документів – у залежності від максимального рівня доступу бази.

Значення за умовчанням політики аудита обрано таким чином, щоб у журналі реєструвались всі події, важливі з точки зору захисту інформації, а, з іншого боку, не реєструвались малозмістовні події, які лише захаращують журнал. Змінювати це значення рекомендується тільки в особливих випадках (наприклад, у разі виникнення обставин, які вказують на можливий витік секретної інформації).

Лабораторна робота № 10
Встановлення політики блокування облікового запису. Встановлення політики паролів

Мета роботи: отримання досвіду конфігурації комплексу засобів захисту при втсановленні блокування облікового запису.

Завдання лабораторної роботи

На автоматизованій системі класу 1, де встановлено комплекс засобів захисту «Лоза-1», ввійти під обліковим записом «Адміністратор безпеки» та здійснити налаштування згідно нижчезаначеної методики.

10.1 Політика блокування облікового запису

Політика блокування облікового запису використовується для підвищення стійкості до підбору паролів. Вона визначається такими параметрами конфігурації системи:

- інтервал для поновлення відліку невдалих спроб входу до системи;
- максимальна кількість невдалих спроб входу до системи.

Параметр максимальна кількість невдалих спроб входу до системи вказує кількість невдалих спроб входу до системи, після яких обліковий запис блокується. Як невдалі спроби входу зараховуються всі спроби входу, спроби розблокування комп’ютера та спроби зміни пароля, під час яких користувач вказує невірний пароль.

Параметр інтервал для поновлення відліку невдалих спроб входу до системи визначає інтервал, після закінчення якого відлік невдалих спроб входу поновлюється.

Політика блокування облікового запису застосовується тільки в тому випадку, коли для параметра дозволяти вхід до Windows тільки користувачам системи задане значення *Так*

10.2 Встановлення політики паролів

Політика паролів використовується для підвищення стійкості до підбору паролів. Вона визначається такими параметрами конфігурації:

- кількість неповторюваних паролів;
- максимальний термін дії пароля;
- мінімальна довжина пароля;
- паролі повинні задовольняти вимогам щодо складності.

Параметр кількість неповторюваних паролів обмежує можливість користувачів використовувати старі паролі під час зміни пароля.

Параметр максимальний термін дії пароля визначає термін, після закінчення якого система змушує користувача змінити пароль.

Параметр мінімальна довжина пароля не дозволяє використовувати занадто короткі паролі.

Параметр *паролі* повинні задовольняти вимогам щодо складності змушує користувача використовувати досить складні паролі. Складність пароля означає виконання таких вимог:

- пароль не повинен містити в собі ім’я або повне ім’я користувача;

- пароль має містити символи хоча б із трьох наборів із наведених чотирьох:

  - прописні літери латинського, російського та українського алфавітів;
  - строкові літери латинського, російського та українського алфавітів;
  - цифри;
  - спеціальні символи: ~ ` ! @ # $ % ^ & * ( ) _ - + = | \ { }

Політика паролів застосовується тільки в тому випадку, коли для параметра *дозволяти вхід до Windows тільки користувачам системи* задане значення *Так*.

Література

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем Київ : БХВ, 2009, 596 с.

2. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации. Том 1. Несанкционированное получение информации Киев : Арий 2008, 326 с.

3. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации. Том 2. Информционная безопасность Киев : Арий 2008 385 с.

4. «Гриф-ХР» Комплекс средств защиты информации от несанкционированного доступа. http://exam.nuwm.edu.ua/pluginfile.php/97261/mod_resource/content/1/gxp_103i.pdf

5. Система захисту інформації «Лоза» http://avtoprom.kiev.ua/avtoprom/ua/content/Система-захисту-інформації-ЛОЗА™-1-версія-4