Міністерство освіти і науки України
Вінницький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту з дисципліни
«Проектування комплексних систем захисту інформації»
для студентів спеціальності 7.160104 “Адміністративний менеджмент
у сфері захисту інформації з обмеженим доступом”

Вінниця ВНТУ 2009

Міністерство освіти і науки України
Вінницький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту з дисципліни
«Проектування комплексних систем захисту інформації»
для студентів спеціальності 7.160104 “Адміністративний менеджмент
у сфері захисту інформації з обмеженим доступом”

Затверджено Методичною радою Вінницького національного технічного університету як методичні вказівки для студентів спеціальності 7.160104 “Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом”. Протокол № 7 від 19 березня 2009р.

Вінниця ВНТУ 2009

Методичні вказівки до виконання курсового проекту з дисципліни «Проектування комплексних систем захисту інформації» для студентів спеціальності 7.160104 “Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом”./ Уклад. С. М. Цирульник, – Вінниця: ВНТУ, 2009. – 46 с.

Рекомендовано до видання Методичною радою Вінницького національного технічного університету Міністерства освіти і науки України.

У методичних вказівках розглянуто особливості проектування комплексних систем захисту інформації. Проектування комплексних систем захисту інформації полягає в тому, щоб для заданого об'єкта створити заданий рівень захищеності інформації при мінімальних витратах на захист або максимально можливий рівень захищеності при заданому рівні витрат на захист. Методичні вказівки розроблено відповідно до плану кафедри обчислювальної техніки і програми дисципліни «Проектування комплексних систем захисту інформації» для спеціалістів в галузі інформаційної безпеки.

Укладач Сергій Михайлович Цирульник

Редактор В. О. Дружиніна

Коректор З. В. Поліщук

Відповідальний за випуск зав.кафедри ОТ О. Д. Азаров

Рецензенти: С. В. Павлов, доктор технічних наук, професор
О. П. Войтович, кандидат технічних наук, доцент

ЗМІСТ

1 ТЕМАТИКА ТА ЗМІСТ КУРСОВОГО ПРОЕКТУ

Проектування систем захисту інформації полягає в тому, щоб для заданого об'єкта створити оптимальні механізми забезпечення захисту інформації та механізми керування ними. Оптимальність систем захисту – це досягнення заданого рівня захищеності інформації при мінімальних витратах на захист або максимально можливого рівня захищеності при заданому рівні витрат на захист. Вибір тієї або іншої постановки задачі залежить від характеру об'єкта, який захищається, від характеру таємниці, яка знаходиться на об'єкті.

При цьому для тих видів секретів, для яких можуть бути визначені розміри втрат при порушенні захисту відповідної інформації, максимально припустимим рівнем витрат на захист буде саме розмір потенційно можливих втрат. Для тих же видів секретів, можливі втрати від розкриття яких не можуть бути виражені вартісними показниками, необхідний рівень захисту повинен визначатися, виходячи з більш загальних показників важливості відповідної інформації.

При вивченні курсу «Проектування комплексних систем захисту інформації» є виконання курсового проекту.

Мета курсового проекту – поглиблення теоретичних знань з дисципліни, надбання навичок з розробки технічних рішень і вміння застосовувати методи проектування систем захисту з урахуванням сучасних тенденцій.

У процесі курсового проекту студент:

- поглиблює і розширює свої знання з ряду дисциплін, які відносяться до теми проекту;
- навчається свідомо і критично підходити до розв'язування технічних задач;
- знайомиться з новітніми технічними ідеями і рішеннями;
- виявляє свої схильності і спроможності в розробці технічних рішень та застосуванні методів проектування;
- одержує досвід у логічному і літературному викладі технічної думки та захисту висунутих ним положень;
- освоює методику оформлення проектних матеріалів і технічних документів;
- набуває навичок, що необхідні для роботи над дипломним проектом.

Курсовий проект є самостійною роботою і виконується кожним

студентом відповідно до завдання, номер якого визначає тип системи захисту інформації, що розробляється і вибирається відповідно до таблиці 1.

Таблиця 1 – Тип системи захисту, що розробляється

Номер завдання	Початкова буква прізвища студента	Категорія системи, що розробляється
1	А, Б, В, Г, Д, Е, Є, Ж, З, И, І	І категорія
2	Ї, Й, К, Л, М, Н, 0, П, Р, С, Т	ІІ категорія
3	У, Ф, Х, Ц, Ч, Ш, Щ, Ю, Я	ІІІ категорія

Номер варіанта вибирається відповідно до останньої цифри залікової книжки студента (таблиця 2).

Таблиця 2– Категорія об'єкта захисту, що розробляється

Категорія об'єкта	Номер варіанта									
	01	02	03	04	05	06	07	08	09	00
А					*			*		
В		*		*		*			*	
С			*				*			*
Опис об'єкта:										
Кабінет керівника об'єкта	*					*				
Науково – дослідна лабораторія		*					*			
Зал засідань			*					*		
Обчислювальний центр				*					*	
Випробувальна ділянка					*					*

Об'єкт захисту – це будівля до 5 приміщень, без прилеглої території, штат до 50 чоловік персоналу, засоби обчислювальної техніки (ЗОТ) до 20 одиниць, до 2 виділених серверів локальної мережі. Одне виділене приміщення (площа не більше 100 кв. м) з 1-2 об'єктами обчислювальної техніки, що включають засоби телефонізації, копіювальної техніки і ін. (далі ООТ).

Характеристики об'єкта уточнюються відповідно до передостанньої цифри залікової книжки студента (таблиця 3).

Як об'єкт, для якого розробляється проект комплексного захисту, можна узяти підприємство (погоджується з керівником курсового проекту), на якому проводилась виробнича практика. При цьому можна скористати-

ся звітом з практики.

Таблиця 3 – Характеристика об’єкта захисту

Характеристика об’єкта	Номер варіанта									
	10	20	30	40	50	60	70	80	90	00
1-й поверх цегляного будинку, який знаходиться на контрольованій території	*					*				
1-й поверх залізобетонного будинку з підвалом, який знаходиться на межі контрольованої зони		*					*			
3-й поверх 5-поверхового залізобетонного будинку з підвалом на межі контрольованої зони			*					*		
3-й поверх 4-поверхового цегляного будинку, який находиться на межі контрольованої зони				*					*	
2-й поверх 4-поверхового залізобетонного будинку, що стоїть окремо					*					*

У курсовому проекті слід розробити проект комплексної системи захисту об’єкта інформатизації (ОІ), що включає такі підсистеми:

- контролю і управління доступом на об'єкт;
- відеоспостереження (охоронного телебачення);
- охоронно-пожежної сигналізації (ОПС);
- протидії економічному шпигунству (аудіоінформація, некомп'ютерні канали зв'язку, паразитні електромагнітні випромінювання і наведення - ПЕМВН і інше);
- захисту корпоративної мережі (внутрішньої та зовнішньої, електронного документообігу, антивірусного захисту - АВЗ, міжмережеві екрани і інше).

2 ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

2.1 Загальні правила оформлення

Пояснювальна записка до курсового проекту оформляється згідно з методичними вказівками до оформлення курсових проектів (робіт) у Вінницькому національному технічному університеті за діючими стандартами України.

Всі підрозділи пояснювальної записки виконують з абзацу малими літерами, починаючи з великої, за винятком змісту і додатків, які виконують посередині рядка великими літерами.

Здавати необхідно оформлену пояснювальну записку і електронну копію. Текст і рисунки (структурні і функціональні схеми) виконувати в редакторові *Word XP,* шрифт *Times New Roman 14*. Орієнтовна кількість листів – 40 (без додатків).

2.2 Структура пояснювальної записки

Пояснювальна записка повинна відповідати індивідуальному завданню, а її оформлення – чинним державним стандартам, які слід враховувати на момент виконання розробки з врахуванням всіх офіційних змін, введених в дію.

Пояснювальна записка повинна мати таку структуру

1. *Вступна частина*, яка містить:
   - титульний аркуш;
   - індивідуальне завдання;
   - анотацію;
   - зміст.
2. *Основна частина*, яка складається з:
   - вступу;
   - опису об'єкта інформатизації, що захищається;
   - політики інформаційної безпеки;
   - переліку інформації, що складає комерційну таємницю;
   - системи контролю і управління доступом на об'єкті (СКУД);
   - системи охоронного телебачення (СОТ);
   - системи охоронно-пожежної сигналізації (ОПС);
   - протидії економічному шпигунству (ПЕШ);
   - комплексу захисту корпоративної мережі (КЗКМ);
   - висновків;
   - літератури.

3. *Додатки*, які розміщуються після основної частини пояснювальної записки курсового проекту.

2.3 Вміст вступної частини пояснювальної записки

2.3.1 Титульний аркуш

Титульний аркуш є першою сторінкою, який не нумерується. Згідно з діючим стандартом ГОСТ 2.105-95 титульний аркуш виконується за встановленим зразком. Зразок титульного аркуша наводиться у додатку А.

На титульному аркуші для курсових проектів подаються:

- тема;
- запис „Пояснювальна записка …" із зазначенням спеціальності, цифрового коду кафедри.

Перераховується науковий ступінь та звання керівника. Підписи керівника та студента із зазначенням термінів обов'язкові.

Запис „нормоконтроль" на титульному аркуші не вказується, але підпис нормоконтролера ставиться в графічній частині проекту та в основному надписі пояснювальної записки (1-й аркуш змісту).

Також на титульному аркуші після захисту курсового проекту має бути виставлена оцінка за лінгвістичною шкалою з підписами керівника та викладача (-ів), що входять до складу комісії.

Робота, яка подається у вигляді копії, до захисту не приймається, у випадку прийняття такої роботи відповідальність несуть керівник та викладач, що входять до складу комісії.

Для курсового проекту титульний аркуш виконується з рамкою.

2.3.2 Індивідуальне завдання

Конкретний зміст кожного курсового проекту, етапи виконання визначає керівник на підставі індивідуального завдання, затвердженого завідувачем кафедри.

Попередньо керівник видає індивідуальне завдання до курсової роботи. Індивідуальне завдання в перелік змісту не вноситься та має бути другою сторінкою після титульного аркуша. Зразок індивідуального завдання до курсового проекту наведено в додатку Б.

Керівник роботи пропонує зміст пояснювальної записки, як правило, в розроблених методичних вказівках або зміст може висвітлюватись в індивідуальному завданні в навчальних цілях.

У залежності від специфіки дисципліни керівник курсового проекту може пропонувати тему, яка підлягає конкретному обґрунтуванню та роз-

робці індивідуального завдання. Індивідуальне завдання до курсового проекту має містити термін видачі, підписи керівника та студента.

Завдання на курсовий проект повинно бути підготовлено не пізніше другого тижня з початку навчального семестру, підписано викладачем, який видав завдання і студентом, що прийняв його до виконання.

2.3.3 Анотація

Анотація призначена для ознайомлення з текстовим документом курсового проекту. Анотація повинна коротко характеризувати мету проекту, засоби, що використані для досягнення поставленої задачі, коротку інформацію про досягнуті результати. Розмір анотації повинен становити приблизно 1/3 частини сторінки.

Анотацію розміщують безпосередньо за аркушем з індивідуальним завданням, починаючи з нової сторінки (третьої), нумерація якої не зазначається.

2.3.4 Зміст

Зміст розташовують безпосередньо після анотації, починаючи з нової сторінки. До змісту включають: вступ; послідовно перелічені назви всіх розділів, підрозділів, пунктів і підпунктів (якщо вони мають заголовки) роботи; висновки; перелік літературних джерел; назви додатків і номери сторінок, які містять початок матеріалу. Зміст не включає титульний лист, індивідуальне завдання на курсовий проект та анотацію. Нумерація у змісті починається зі вступу (відповідно до нумерації у пояснювальній записці). Сам зміст за нумерацією пояснювальної записки є четвертою сторінкою. Нумерація сторінок повинна бути наскрізною.

Назви заголовків змісту повинні однозначно відповідати назвам заголовків пояснювальної записки за текстом. Формування змісту у текстовому документі бажано формувати автоматично, використовуючи засоби обраного текстового редактора.

Для запобігання плутанині з назвами розділів, підрозділів і нумерацією сторінок, а також для полегшення редагування і внесення змін в основний текст пояснювальної записки рекомендується використовувати можливості автоматичного формування змісту у документах Ms Word.

Приклад оформлення змісту можна бачити у даних методичних вказівках.

2.4 Вміст основної частини

2.4.1 Вступ

Відповідно до вибраного прикладного призначення об'єкта слід навести короткий зміст "Переліку відомостей, що складають комерційну (службову) таємницю" і "Положення про комерційну (службову) таємницю", зокрема – мету захисту інформації, необхідний рівень захищеності інформації, основні методи досягнення мети захисту, політику безпеки інформації підприємства.

Виходячи з прикладного призначення об’єкта інформатизації слід обґрунтовано вибрати (рекомендувати до застосування):

- клас захищеності автоматизованої системи (АС), що проводить зберігання і обробку конфіденційної інформації на об'єкті інформатизації;
- клас захищеності засобів обчислювальної техніки (ЗОТ), складових апаратно-програмної підтримки автоматизованої системи;
- клас міжмережевих екранів (МЕ) за рівнем захищеності від несанкціонованого доступу (НСД), що реалізовують захист внутрішньої обчислювальної мережі об’єкта інформатизації;
- клас антивірусних засобів, що використовуються на об’єкті інформатизації;
- рівень контролю програмного забезпечення засобів захисту інформації.

У проекті слід використовувати сертифіковані засоби і системи, що пройшли сертифікацію, не нижче вибраних класів.

2.4.2 Опис об’єкта інформатизації, що захищається

Аналіз технічної оснащеності включає план підприємства і технічний паспорт об'єкта. План підприємства виконується з вказівкою розміщення автоматизованих робочих місць (АРМ), серверів, комутаційного устаткування, ліній зв'язку, електропостачання, заземлення, сигналізації, оргтехніки і інших елементів інформаційної системи підприємства. Технічний паспорт є таблицею, форма якої подана у таблиці 4.

Графи, які є неактуальними для даного об’єкта, дозволяється не заповнювати. Графи для опису різних моделей пристроїв або програмного забезпечення повинні повторюватися.

Таблиця 4 – Технічний паспорт об'єкта

Найменування об'єкта	*Опис об'єкта*
Поверх (поверхів у багатоповерховій будівлі)	
Наявність сховищ паперових документів	Скільки? Які кімнати?
Наявність кімнат з неконтрольованим доступом	Скільки? Які?
Порядок доступу в приміщення	Які кімнати і як здаються під охорону?
Наявність інших підприємств	Так /ні?
Склад технічних засобів	
Кількість і технічні характеристики серверів	Тип процесора, материнської плати, об'єм ОЗП, об'єм жорсткого диска, операційна система (ОС)
Кількість і характеристики АРМ	Тип процесора, материнської плати, об'єм ОЗП, об'єм жорсткого диска, монітор, ОС
Кількість і характеристики терміналів	Тип процесора, материнської плати, об'єм ОЗП, об'єм жорсткого диска, монітор, ОС
Кількість комутаторів локальної обчислювальної мережі (ЛОМ)	виробник, модель, продуктивність, кількість портів
Вихід до Internet	
Тип підключення	(Dial-Up/ADSL/комутований канал), швидкість передачі
Комунікаційне устаткування	виробник, модель
Комунікаційне програмне забезпечення	Шлюз, мережевий екран
Характеристика програмного забезпечення (ПЗ)	
Інформаційне ПЗ	
Тип ПЗ	Мережеве? (так/ні), кількість місць
Структура ПЗ (Клієнт-сервер/Файл-сервер)	Виробник, версія
Обсяг бази даних	
Додаткове ПЗ	
Найменування	Призначення, версія, мережеве? (так/ні)
Додаткове устаткування	
Факси	Виробник, модель, кількість

Продовження таблиці 4

Найменування об'єкта	*Опис об'єкта*
Факс-модеми, що не використовуються для Internet	Виробник, модель, кількість
Внутрішня автоматична телефонна станція (АТС)	Виробник, модель, кількість
Телефони	Виробник, модель, кількість

2.4.3 Перелік інформації, що складає комерційну таємницю

Перелік включає перерахування інформації, яка в рамках даного підприємства має конфіденційний характер (складають службову або комерційну таємницю). Конфіденційна інформація у переліку групується по структурних підрозділах компанії (відділах, службах). Указується можливий збиток у результаті несанкціонованого розповсюдження інформації, яка включена до переліку. Визначаються переваги закритого використання інформації у порівнянні з відкритим. Оцінюються витрати на захист даної інформації.

2.4.4 Політика інформаційної безпеки

Документ призначений для керівництва і містить:

- основні положення, що стосуються інформаційної безпеки підприємства;
- перелік найбільш характерних загроз;
- моделі порушників безпеки;
- пріоритетні заходи щодо реалізації політики інформаційної безпеки, що включають перелік необхідних засобів інформаційного захисту;
- адміністративні аспекти забезпечення безпеки (порядок призначення відповідальних осіб, облік розподілу паролів ідентифікаторів, дії адміністрації при спробах несанкціонованого доступу).

2.4.5 Система контролю і управління доступом на об’єкт

У даному розділі пояснювальної записки повинні міститися короткі відомості про оснащення одного з блоків захисту (виділена територія, будівля, поверх, група приміщень) системою управління доступом.

Структура об'єкта інформатизації, що захищається

1. Структура розташування блоків, що захищаються, приміщень або зон, розміщення прохідних, приміщень для розташування АРМ управління.

2. Найменування об'єктів, що підлягають оснащенню системою контролю і управління доступом (адміністративні, виробничі, складські, побутові приміщення, виробничі майданчики або внутрішні території з КПП).

3. Структура частини (блока) об'єкта інформатизації, що захищається. Кількість окремих об'єктів (перелік об'єктів, що захищаються, окремих будівель, виділених поверхів, груп приміщень).

4. Вказати, які завдання розв’язуються системою, наприклад:

- контроль і управління доступом співробітників і відвідувачів на територію об'єкта;
- контроль і управління доступом співробітників і відвідувачів до одного або ряду будівель, приміщень;
- контроль і управління в'їзду\ виїзду транспорту (авто, залізничного, спеціального) через КПП об'єкта;
- автоматичне ведення баз даних проходів в межах об'єкта, що захищається.

5. Кліматичні умови в районі розташування об'єкта. Температурний режим, глибина промерзання ґрунту, сейсмічність.

Користувачі системи

1. Загальна кількість користувачів системи, максимальна кількість співробітників, відвідувачів, одиниць транспорту.

2. Тип ідентифікаторів користувачів: перепустка, магнітні, дистанційні (*Proximity*) або контактні (*Touch Memory*) карти.

3. Необхідність розміщення на ідентифікаційному посвідченні фотографії співробітника, логотипа компанії і тому подібне

4. Необхідність в оснащенні бюро перепусток комплексом для оперативного виготовлення ідентифікаційних посвідчень з фотографіями користувачів, іншим спеціальним устаткуванням.

Прохідні об'єкта

1. Загальна кількість прохідних і контрольно-пропускних пунктів (КПП) для транспорту, що включаються до складу СКУД.

2. Максимальне навантаження на кожну прохідну – людин за годину (необхідна для розрахунку кількості турнікетів або інших засобів управління доступом).

Корпоративна мережа і АРМ служби охорони об'єкта

1. Кількість і розташування автоматизованих робочих місць (АРМ) для управління СКУД (АРМ адміністратора безпеки, АРМ служби охорони, АРМ бюро пропусків, АРМ служби персоналу, інші АРМ).

2. Необхідність взаємодії АРМ управління різних об'єктів.

3. Наявність корпоративної мережі, яка зв'язує об'єкти (АРМ системи управління доступом повинні розташовуватися в межах ЛОС).

4. Структура корпоративної мережі, наявність виділених каналів передачі даних, телефонної мережі для СКУД.

5. Захист АРМ СКУД від несанкціонованого доступу.

6. З якими АРМ необхідно забезпечити взаємодію в реальному масштабі часу (перелік АРМ, що взаємодіють)?

Можливість інтеграції з іншими системами

1. Можливість інтеграції системи із засобами забезпечення безпеки комп'ютерних систем: на яких комп'ютерах, АРМ, серверах, об'єктах обчислювальної техніки.

2. Взаємодія СКУД із засобами відеоспостереження і відеореєстрації, з системами охоронної сигналізації.

3. Вимоги сумісності і умови сумісності з виконавчими пристроями (турнікетами, тамбур-шлюзами у вигляді дверей, автоматичними, напівавтоматичними шлюзовими кабінами); системами відеоспостереження; охоронно-пожежної сигналізації; системою сповіщення і ін.

4. Вимоги сумісності з технологічним устаткуванням, що використовується. Необхідність і умови сумісності з існуючими системами (елементами) технологічного процесу на об'єктах.

Опис роботи системи

1. Короткий опис технології роботи системи (опис загальної тактики проходу, структури й пріоритетності зон, що захищаються, прав і обов'язків охоронців і контролерів КПП і т.п.). Можливість подальшого розширення системи. Додання нових пунктів контролю й нових автоматизованих робочих місць.

2. Короткий опис функціональних можливостей системи контролю й управління доступом. Система повинна забезпечувати:

- реєстрацію й протоколювання тривожних і поточних подій;
- пріоритетне відображення надзвичайних подій;
- керування роботою пристроями, що перекривають рух, у точках доступу за командами оператора;
- завдання тимчасових режимів дії ідентифікаторів у точках доступу, "вікнах часу" і рівнів доступу;
- захист технічних і програмних засобів від несанкціонованого доступу до елементів керування, установлення режимів і до інформації;
- автоматичний контроль справності засобів, що входять у систему, і ліній передачі інформації;
- можливість автономної роботи контролерів системи зі збереженням контролерами основних функцій при відмові зв'язку з пунктом централізованого керування;
- установлення режиму вільного доступу з пункту керування при аварійних ситуаціях і надзвичайних подіях;
- блокування проходу у точках доступу з пункту керування.

3. Особливості технічних, експлуатаційних характеристик і дизайну устаткування, що застосовується, наявність сертифіката відповідності на усе устаткування, яке застосовується.

4. Особливості виконавчих механізмів: типи замків, турнікетів, шлюзових кабін, переговорних пристроїв.

5. Особливості установлення системи:

- розміщення контролерів (за місцем й способом установлення контролерів, підведення інформаційних шлейфів і шин живлення);
- прокладка кабельних трас, тип кабелю, виконання кабельних трас

або коробів (шлангів, труб);

- місця підключення контролерів, блоків керування виконавчими пристроями до розподільного щита ~220В, а також місця вертикальної прокладки кабелів між поверхами.

Окремий блок захисту (будинку, поверху, групи приміщень)

1. Найменування або призначення блока.

2. Кількість користувачів системи в блоці.

3. Кількість приміщень, що захищаються, з розподілом їх по поверхах. Кількість контрольованих дверей.

4. Кількість прохідних, контрольованих входів, КПП для транспорту. Орієнтовне навантаження проходів.

5. Найменування прохідної, виконання прохідних, (турнікети, тамбур-шлюзи у вигляді дверей, шлюзові кабіни автоматичні, шлюзові кабіни напівавтоматичні, шлагбауми, розсувні ворота), їхня кількість.

6. Можливість установлення на прохідних металодетекторів.

7. Можливість протоколізації дій служби охорони з пропуску відвідувачів через прохідну.

8. Указати мету або вимоги до системи відеореєстрації на прохідній.

9. Оснащення блока, приміщення, окремих дверей аудіо- або відеодомофоном для прийому відвідувачів.

10. За кожними дверми індивідуально:

- завантаження проходів на добу (орієнтовно);
- кількість користувачів для даних дверей (орієнтовно);
- наявність і необхідність резервування живлення;
- установлення системи дистанційного відмикання дверей зсередини приміщення для відвідувача, не встаючи з робочого місця, метраж кабелю від дверей до системи дистанційного відмикання (орієнтовний);
- наявність і необхідність доводчика;
- необхідність кнопки відмикання;
- можливість протоколізації проходів користувачів для даних дверей;
- виконання дверей (з дерева, металу, профілю, скла).

11. Наявність ЛОМ у будинку, групі приміщень для організації взаємодії АРМ.

12. Тип операційної системи, структура локальної мережі в межах будинку, групи приміщень.

13. Наявність резервного живлення й загальної шини заземлення в будинку.

Даний розділ пояснювальної записки повинен обов'язково містити:

- структурні схеми (рисунки) об'єкта й одного із блоків захисту з розміщенням устаткування СКУД, схеми корпоративної мережі, схеми виділених ліній зв'язку, що комутуються;
- специфікацію (технічні характеристики) устаткування й програмного забезпечення СКУД (у додатку);
- кошторис витрат оснащення об'єкта системами контролю й керування доступом.

2.4.6 Система охоронного телебачення

У даному розділі пояснювальної записки повинні бути короткі відомості про оснащення системою охоронного телебачення (СОТ) одного із блоків захисту об'єкта (виділена територія, будинок, поверх, група приміщень).

1. Назви й призначення блоків усередині об'єкта інформатизації (виділена територія, будинок, поверх, група приміщення), для яких проектується система відеоспостереження: адміністративні, виробничі, складські, побутові приміщення, виробничі площадки, суміжні або внутрішні території різного призначення.

2. Кількість окремих зон, ділянок, об'єктів, що оснащуються системою (перелік зон, що захищаються, територій, окремих будинків, виділених ділянок). Указати на схемі розташування приміщень, що захищаються, або зон, розміщення постів спостереження. Описати за кожною зоною контролю світлову обстановку або умови видимості, кліматичні умови: температурний режим, глибина промерзання ґрунту, сейсмічність.

3. Мету спостереження в денному й нічному режимі. Наприклад: удень - ідентифікація особи, визначення номера автомобіля, що в'їжджає, уночі - виявлення автомобіля, людини, і т.д. (з наданням планів зон контролю, і прилеглої території).

4. Розв'язувані системою завдання, наприклад:

- контроль несанкціонованого доступу співробітників або порушників на територію (або з території) об'єкта через прохідні й КПП;
- контроль несанкціонованого доступу співробітників або порушників на територію (або з території) об'єкта через огородження або заборонні зони;
- захист людей і матеріальних цінностей від злочинних зазіхань у контрольованій зоні об'єкта охорони;
- контроль за ситуаційним положенням у виділеному приміщенні або на території, що прилягає до об'єкта;
- ідентифікація особистості відвідувача або співробітника об'єкта при проходженні КПП на підставі даних відеотеки;
- ідентифікація державного номера автомашини при проїзді КПП об'єкта на підставі баз даних служби охорони або бюро пропусків;
- контроль за діями співробітників певних служб на об'єкті в ході технологічного процесу або виконання ними своїх службових обов'язків;
- автоматична фіксація й зберігання протягом певного часу запису протиправних або інших подій за надзвичайним повідомленням з об'єкта, що захищається;
- автоматична фіксація й зберігання протягом певного часу (указати розмір архіву на один місяць) усіх подій з об'єкта охорони або території.

Пости спостереження й керування комплексом

1. Кількість незалежних постів спостереження (із вказівкою місць їхнього розміщення на планах).

2. Можливість відеореєстрації на магнітофон тривалого запису: безупинно, за розсудом оператора, за сигналами охоронних датчиків.

3. Можливість одночасного перегляду на одному моніторі всіх відеокамер комплексу: завжди, тільки в режимі безпосереднього спостереження за об'єктом.

4. Можливість виконувати охоронні функції (детектори руху).

5. Можливість моментального роздрукування кадрів, що цікавлять, на відеопринтері.

6. Можливість погодженої роботи комплексу з персональним

комп'ютером (комп'ютерами). У цьому випадку вказати кількість і розташування АРМ відеоспостереження, структуру комп'ютерної мережі на об'єкті.

Опис системи охоронного телебачення

1. Загальні вимоги до системи відеоспостереження:
   - кольорова, чорно-біла, комбінована;
   - термін зберігання відеозаписів в архіві (як правило, один місяць);
   - необхідність у доповненні системи відеоспостереження системою автоматизованого керування доступом у приміщення й на об'єкти;
   - необхідність фіксації аудіоінформації з об'єктів охорони;
   - можливість розширення системи;
   - наявність і розташування щитів електроживлення поблизу місць установлення устаткування й на постах спостереження;
   - наявність резервного або дублювального живлення;
   - можливість подальшого розширення шляхом додавання нових телекамер і постів спостереження (охорони).

2. Технологія роботи системи (опис загальної тактики відображення й записи інформації, структури й пріоритетності зон, що захищаються, порядку й рівня з'єднання із взаємодіючими системами, права і обов'язки охоронців і контролерів КПП і т.д.).

3. Функціональні можливості системи охоронного телебачення.

4. Технічні характеристики системи:
   - роздільність системи (для кожного відеоканалу);
   - час реагування системи на надзвичайну подію (для кожного відеоканалу).

5. Технічні характеристики пристроїв виявлення руху (для кожного відеоканалу, що обладнаний детектором руху):
   - мінімальний діапазон виявлення об'єкта;
   - мінімальний контраст виявлення об'єкта;
   - діапазон швидкостей руху об'єкта.

6. Технічні характеристики пристроїв керування й комутації відеосигналів:
   - роздільність;

- відношення сигнал/шум;
- вид вхідного сигналу повідомлення про тривогу;
- максимальні напруги й струми комутації.

7. Технічні характеристики відеомоніторів:

- роздільність;
- максимальна яскравість зображення;
- геометричні й нелінійні спотворення зображення.

8. Можливості системи по забезпеченню нормальної стабільності від прогнозованих несанкціонованих дій (НСД) і/або можливість розміщення в приміщеннях, місцях (сейфах, боксах і ін.), захищених від:

- руйнуючих механічних НСД;
- несанкціонованого доступу до програмного забезпечення.

9. Можливості системи забезпечувати розмежування прав користувачів/операторів: на програмному й апаратному рівнях.

10. Вимоги системи до електроживлення:

- основне електроживлення системи повинне здійснюватися від мережі змінного струму;
- система (окремі елементи системи) повинна мати резервне живлення (указати вид резервного живлення: за змінним або постійним струмом, указати величину - 12 або 24В, а також час роботи системи (окремих елементів системи) при зникненні основного живлення.

11. Можливість сумісності системи охоронного телебачення з діючими технологіями; необхідність і умови сумісності з існуючими системами (елементами) контролю й керування доступом, охоронно-пожежної сигналізації; системою оповіщення й іншими.

12. Можливість сумісності з технологічним устаткуванням, що використовується; необхідність і умови сумісності з існуючими системами (елементами) технологічного процесу на об'єктах.

13. Інші технічні й експлуатаційні характеристики й дизайн устаткування, що застосовується:

- наявність сертифіката відповідності на усе устаткування, що застосовується;
- особливості відеокамер, квадраторів, мультиплексорів і іншого відеоустаткування за кольором, зовнішнім виглядом відеокамер і іншого устаткування;
- особливості розміщення відеокамер за місцем й способом

установлення відеокамер;

- особливості прокладання кабельних трас: типу кабелю, виконання кабельних трас або коробів (шлангів, труб).

Даний розділ пояснювальної записки повинен обов'язково містити:

- структурну (функціональну) схему розміщення відеокамер на об’єкті, із вказанням мети й місця її установлення, устаткування системи й постів охорони СОТ;
- специфікацію (технічні характеристики) устаткування, що поставляється, і програмного забезпечення (у додатку);
- кошторис витрат оснащення об'єкта системою охоронного телебачення.

2.4.7 Система охоронно-пожежної сигналізації

У даному розділі пояснювальної записки повинні бути короткі відомості про оснащення внутрішньої території об'єкта охорони технічними засобами системи охоронно-пожежної сигналізації (ОПС).

Загальні відомості про об'єкт

1. Перелік і характеристик об'єктів захисту, що потребують обладнання системи автоматичної сигналізації (пожежної, охоронної, охоронно-пожежної): виробничі, складські, житлові, побутові приміщення, відкриті площадки, ділянки, огороджування й інші.

2. Приміщення, що захищаються, віднесені до категорії особливо важливих за типом цінностей, що зберігаються там, або ступеня вибухо-пожежонебезпеки: найменування приміщення або групи приміщень. Типи цінностей, що зберігаються. Необхідність роздільного підключення.

3. Приміщення, у яких потрібне виконання висотних робіт (висотою більше 2,5 метра): найменування приміщення або групи приміщень. Типи цінностей, що зберігаються. Висота приміщення.

4. Приміщення, у яких електромагнітні наводки перевищують допустимий рівень.

5. Наявність на об'єкті систем примусової вентиляції, димозбірника, вогнезатримувальних клапанів у вентиляційних каналах (для пожежної сигналізації).

6. Наявність підвісних стель, з якого матеріалу виконані і чи є за ними пожежне навантаження (більше 5 силових кабелів, крім освітлення).

7. Найбільш уразливі місця для несанкціонованого проникнення на об'єкт; якщо є, то побажання щодо конфігурації охорони об'єкта.

8. Конструктивний матеріал дверей, вікон, воріт.

9. Місце прокладання кабелю між поверхами.

10. Кліматичні умови: температурний режим, глибина промерзання ґрунту, сейсмічність.

Опис периметра території об'єкта, що захищається

1. Найменування й призначення території, що захищається.

2. Що собою являє периметр території, що захищається (наприклад, огороджування, стіна будинку й т.д.).

3. Висота й тип огороджування (бетонне, дерев'яне, сітчасте, металеве, ґрати й т.п.).

4. Наявність зони відчуження або можливість її створення.

5. Загальна довжина периметра, що підлягає захисту, площа території, що захищається (схема).

6. Найменування, призначення суміжних із територією захисту, будинків, споруджень. Їх висота, особливості конструкції.

7. Кількість воріт для проїздів залізничного і автомобільного транспорту, прохідних.

8. Місця й способи складування й зберігання матеріальних цінностей на території, що захищається.

9. Наявність підземних і підвісних комунікацій на території, що захищається.

10. Найбільш уразливі місця для проникнення порушника, ймовірні способи проникнення для конкретного об'єкта (підкоп, перелізання, проламлювання, сусідні будинки, спорудження, тощо).

Живлення системи

1. Джерела електроживлення систем сигналізації. Їх місце установлення (розташування силового щита). Склад джерел живлення системи ОПС:

– змінного струму напругою 220 В, 50 Гц, потужністю 1 кВт

(потрібно два незалежних мережевих джерела для живлення випромінювачів, контрольних панелей і периферійної апаратури);

- акумуляторна батарея;
- блок резервного живлення (БРЖ).

Пости охорони

1. Наявність і розташування приміщення (поста) охорони із цілодобовим чергуванням. Тип існуючого пульта централізованого спостереження (ПЦС) або вимоги до проектованого ПЦС.

2. Чи є необхідність виведення сигналів системи на ПЦС місцевого відділу позавідомчої охорони (міліції). У цьому випадку вибір устаткування обмежений дозволеним переліком.

3. Наявність і кількість телефонних пар, місце розташування телефонної коробки (для випадку з передачею сигналу на ПЦС).

4. Місце установлення, що рекомендується, приймально-контрольного приладу (у випадку відсутності приміщення охорони із цілодобовим чергуванням).

5. Указати найменування й розташування приміщення із цілодобовим чергуванням обслуговуючого персоналу, місце, куди системою видаються сигнали.

6. Указати найменування організації, спосіб передачі, типи й адреси ліній зв’язку для видачі дублюючих сигналів.

Функціональні можливості системи

1. Технологія роботи системи: опис загальної тактики охорони, структури й пріоритетності зон, що захищаються.

2. Опис тактики охорони:

- захист системи від несанкціонованого доступу кваліфікованого зловмисника;
- опис видів сигналів, що видаються системою на об’єкті захисту, у приміщенні охорони, в інших органах або організаціях, наприклад, "Прийнятий під охорону", "Знятий", "Тривога", "Пожежа", "Несправність", "Злом" і інші.

3. Можливості розширення системи, нарощування технічних і функціональних можливостей, вимог до надійності, резервування за

живленням, сигнальними лініями зв'язку.

4. Особливості функціонування системи: опис додаткових вимог, наприклад, до звукових і світлових сигналів і інше.

Сумісність системи ОПС

1. З якими існуючими системами сигналізації повинна спільно працювати система, що розробляється.

2. Сумісність із діючими технологіями (опис вимог до підключення системи, що проектується в діючий комплекс технічних засобів охорони).

3. Сумісність із технологічним устаткуванням, що використовується, будівельними конструкціями, будинками, спорудами й т.д. (опис вимог за узгодженням функціонування системи, що проектується, й діючих систем відеоспостереження, контролю й управління доступом, систем керування технологічним устаткуванням).

Інші особливості системи ОПС

1. Особливості технічних і експлуатаційних характеристик і дизайну устаткування, що застосовується.

2. Особливості розміщення випромінювачів, контрольних панелей і лінійно-кабельних споруд.

3. Необхідність узгодження проекту об'єкта системою автоматичної сигналізації в органах (пожежної, охоронної, охоронно-пожежної, позавідомчої охорони МВС, служби безпеки об’єкта інформатизації).

Даний розділ пояснювальної записки повинен обов'язково містити:

- структурні схеми (рисунки) системи захисту, території об'єкта з розміщенням устаткування ОПС;
- специфікація (технічні характеристики) устаткування ОПС (у додатку);
- кошторис витрат оснащення об'єкта устаткуванням ОПС.

2.4.8 Система протидії економічному шпигунству

Загальні відомості про об’єкт, що захищається

1. Список і місце розташування (будинок, поверх) приміщень, що

підлягають оснащенню системою протидії економічному шпигунству. До таких приміщень можуть відноситись:

- виділені приміщення, що призначені для ведення особливо секретних переговорів і нарад;
- кабінети керівництва й інші приміщення, у яких проводяться конфіденційні переговори й наради;
- інші технологічні приміщення, у яких циркулює інформація, призначена для службового користування.

2. Визначення каналів зв'язку, що підлягають захисту:

- виділені канали, що призначені для передачі особливо секретної інформації;
- канали, по яких передається конфіденційна інформація;
- канали, по яких передається інформація для службового користування.

3. Заявлена ступінь конфіденційності (таємності), що циркулює на об'єкті захисту: система повинна забезпечувати клас захисту інформації не нижче класу захищеності АС для об'єктів інформатизації.

4. Площа приміщень об'єкта, що захищається, (кв.м).

5. Тип зовнішніх стін, міжповерхового перекриття (стеля, підлога), (капітальні: бетонні товщиною більше 200 мм або цегельні товщиною більше 500 мм).

6. Входи в приміщення. Тамбури (подвійні двері), відстань між дверима. Двері: тип конструкції, наявність ущільнення, запорні пристрої.

7. Вікна: кількість прорізів, тип засклення, наявність і тип захисних плівок.

8. Тип і висота стель (м): підвісні із зазором, підшивні, оштукатурені, інші.

9. Опис суміжних приміщень, що примикають до стін об'єкта, над і під об'єктом. Призначення приміщень або характер проведених у них робіт.

10. Організація контролю й керування доступом на об'єкті у цілому й у виділеному приміщенні.

11. Наявні на об'єкті засобу зв'язку: користувачі засобів зв'язку, стандарт або принцип дії, найменування або тип апаратури, кількість каналів. У тому числі лінії телефонного зв'язку: кількість вхідних ліній міської й внутрішньої телефонної мережі.

12. Система електроживлення й освітлення: джерела живлення,

розташування трансформаторної розв'язки.

13. Система заземлення: наявність, структура контуру заземлення, опір.

14. Системи сигналізації (тип).

15. Інші провідні лінії: радіотрансляція (місцева, міська), електрочасофікація (марка).

16. Наявність спеціальних технічних засобів захисту інформації.

17. Схема приміщення й розташування в ньому меблів і інших предметів інтер'єру (із вказанням основних розмірів або масштабу). Опис обстановки навколо об’єкта захисту

18. Опис сусідніх будівель: призначення (характер робіт, що там проводяться), поверховість, відстань до приміщення, що захищається.

19. Наявність і віддаленість автостоянки.

20. Архітектурні або технічні особливості приміщень, що захищаються, особливості розташування приміщень усередині будинку.

21. Система вентиляції на об’єкті (тип).

22. Система опалення.

23. Наявна оргтехніка.

24. Наявна побутова техніка: телебачення (марка телевізора), кабельне телебачення, антена зовнішня (кімнатна).

Аналіз інформаційних загроз

1. Визначення видів інформаційних загроз у приміщеннях і технічних каналах.

Із проникненням на об'єкт:

- впровадження спеціальних пристроїв з метою перехоплення інформаційних сигналів, їхнього перетворення й передачі за межі зони безпеки об'єкта по різних каналах;
- несанкціонований запис інформаційних сигналів з використанням засобів реєстрації інформації.

Без проникнення на об'єкт:

- для прослуховування каналів зв'язку,
- навмисний розрив каналів зв'язку,
- для перехоплення залишкових інформаційних сигналів і електромагнітних випромінювань, що поширюються за межі зони безпеки об'єкта.

2. Визначення видів інформації, що перехоплюється, в основних каналах витоку інформації:

- акустичний канал - мовні та інші акустичні сигнали;
- віброакустичний канал - мовні та інші акустичні сигнали;
- витік по провідному каналу - мовні та інші акустичні сигнали, факсимільна, телеграфна, телетайпна інформація, інформація, що обробляється на ЕОМ, або передана модемними каналами;
- електромагнітні поля - інформація передана по радіотелефону й радіозв'язку, інформація, передана по радіомодему;
- ПЕМВН - інформація, що обробляється на ЕОМ, ПЕМВН іншого офісного устаткування, яка промодульована корисним акустичним сигналом;
- оптичний - прихована фото-, кіно- й відеозйомка, відеоспостереження поза зоною охорони.

3. Оцінка оперативно-тактичних можливостей порушника. Формування моделі порушника, його можливостей з:

- перехоплення інформації в безпосередній близькості від території об'єкта;
- легального проникнення на територію об'єкта, наприклад, мати статус співробітника філіалу підприємства або клієнта;
- тимчасового використання або стаціонарного установлення технічних засобів промислового шпигунства;
- одержання апріорних даних, що можуть полегшити планування й проведення операцій з перехоплення інформації.

До таких даних відносяться, наприклад:

- тематика інформації, що перехоплюється;
- інформація про перелік розв'язуваних питань;
- технічні засоби зберігання, обробки й передачі інформації, загальні параметри сигналів, що несуть корисну інформацію;
- розташування приміщень;
- організація й технічна оснащеність служби безпеки,
- розпорядок роботи об'єкта;
- психологічна обстановка в колективі.

4. Оцінювання технічного оснащення порушника за наступними групами технічних засобів перехоплення й реєстрації інформації.

Радіомікрофони (перехоплення акустичної інформації),

- без стабілізації каналу передачі;
- зі стабілізованим каналом передачі;
- з кодованим каналом передачі;
- з акустичним автоматом.

Телефонні радіопередавачі (перехоплення телефонної інформації):

- з не стабілізованим каналом;
- зі стабілізованим каналом;
- безконтактні ємнісні передавачі,
- безконтактні індукційні передавачі,
- передавачі комбіновані (телефонно-акустичні).

Диктофони-адаптери (перехоплення телефонних переговорів):

- контактні;
- безконтактні.

Системи кабельних мікрофонів (перехоплення акустичної інформації):

- системи з передачею "відкритого" сигналу;
- системи з передачею кодованого сигналу;

Системи з передачею інформації з мереж електроживлення й телефонних ліній (перехоплення акустичної інформації).

Спрямовані мікрофони (перехоплення акустичної інформації):

- лінійні;
- параболічні;
- "лазерні детектори".

Комплекси для перехоплення інформації з монітора ЕОМ у реальному часі.

Стетоскопи (перехоплення акустичної інформації):

- провідні,
- з передачею інформації по радіоканалу.

Апаратура для перехоплення залишкових інформативних сигналів у лініях живлення й заземлення.

Апаратура для перехоплення радіоефірної інформації й ПЕМВН офісного устаткування:

- широкосмугові сканувальні радіоприймачі (перехоплення радіопереговорів);

- селективні мікровольтметри (перехоплення корисної інформації, що зберігається у ПЕМВН офісного устаткування).

Апаратура звукозапису (перехоплення акустичної інформації):

- диктофони й магнітофони (запис на міні- і мікрокасету),
- цифровий диктофон.

5. Оцінювання технічних можливостей потенційного порушника з врахуванням його фінансового становища й доцільності вкладення засобів у конкретну операцію з перехоплення інформації. Звичайна кількість вкладених коштів пропорційно вартості інформації, що цікавить порушника.

Функції спеціального устаткування

1. Захист від витоків інформації по акустичному каналу, за рахунок: ПЕМВН засобів обчислювальної техніки і звукопідсилювальної апаратури, по колах живлення й заземлення, по каналах візуального спостереження, віброакустичному каналу.

2. Захист від витоків по провідних каналах - мовні та інші акустичні сигнали, факсимільна, телеграфна, телетайпна інформація, інформація, що обробляється на ЕОМ, або передана по модемних каналах.

3. Захист від витоків через електромагнітні поля - інформація передана по радіотелефону й радіозв'язку, інформація, передана по радіомодему.

4. Захист від витоків через ПЕМВН - інформація, що обробляється на ЕОМ, ПЕМВН іншого офісного обладнання, що промодульований корисним акустичним сигналом.

5. Захист від витоків через оптичний канал - прихована фото-, кіно- й відеозйомка, відеоспостереження поза зоною охорони.

Технологія роботи системи ПЕШ

1. Система захисту інформації повинна забезпечувати оперативне й непомітне виявлення активних радіомікрофонів, що занесені у приміщення, які мають традиційні канали передачі інформації.

2. Система захисту інформації повинна забезпечувати протидію виявленим радіомікрофонам із традиційним каналом передачі інформації.

3. Апаратура системи захисту інформації по акустичному й вібро-

акустичекому каналу повинна включатися в роботу за командою оператора.

4. Вмикання апаратури захисту інформації від знімання з використанням записувальних пристроїв повинно управлятися оператором.

5. Система захисту інформації повинна забезпечувати протидію перехопленню інформації, що передається по телефонній лінії (на ділянці до АТС).

Функціональні можливостям системи ПЕШ

Система повинна забезпечувати захист інформації від витоків:

- через акустичний канал з використанням різної звукозаписувальної апаратури, що внесена на об'єкт;
- через акустичні канали у вигляді мембранного перенесення мовних сигналів через перегородки за рахунок малої маси й слабкого загасання сигналів;
- через акустичні канали за рахунок слабкої акустичної ізоляції (щілини стояків системи, опалення, вентиляція);
- через віброакустичний канал за рахунок поздовжніх коливань конструкцій огороджування й арматури систем опалення;
- через провідний канал від знімання інформації з телефонної лінії (міська й внутрішня телефонна мережа, факсимільний зв'язок, переговорні пристрої, системи конференц-зв'язку й оповіщення, системи охоронної й пожежної сигналізації, мережі електроживлення й заземлення);
- через канал електромагнітних полів основного спектра сигналу за рахунок використання різних радіомікрофонів, телефонних радіопередавачів;
- через оптичні канали за рахунок візуального спостереження за об'єктом з використанням технічних засобів;
- через канали ПЕМВН за рахунок модуляції корисним сигналом електромагнітних полів, що утворяться при роботі побутової техніки;
- через канали ПЕМВН при обробці інформації на ПК за рахунок паразитних випромінювань комп'ютера.

Стаціонарні засоби захисту інформації

1. Визначення стаціонарних засобів захисту інформації у виділеному приміщенні для проведення переговорів і нарад. Звичайно використовуються такі види технічних засобів:

- система, що блокує передачу інформації з мережі живлення;
- засіб блокування віброканалу;
- визначник працюючих диктофонів;
- подавлювач радіомікрофонів і диктофонів;
- генератори акустичного шуму;
- стаціонарний детектор електромагнітного поля.

2. Визначення стаціонарних засобів захисту інформації в кабінетах керівництва й приміщеннях, у яких проводяться переговори й наради. Звичайно використовуються такі види технічних засобів:

- комплексний генератор шуму;
- система вібродатчиків;
- виявник працюючих диктофонів;
- подавлювач радіомікрофонів і диктофонів;
- генератори акустичного шуму;
- стаціонарний індикатор електромагнітного поля;
- фільтри для провідних ліній.

3. Визначення стаціонарних засобів захисту інформації в інших технологічних приміщеннях, у яких циркулює інформація, призначена для службового користування. Звичайно використовуються такі види технічних засобів:

- фільтри для провідних ліній;
- при наявності в приміщеннях ПЕМВН повинні бути встановлені генератори радіоелектронного шуму (у варіанті захисту робочого місця).

4. Визначення стаціонарних засобів захисту інформації у виділених каналах зв'язку для передачі:

- особливо секретної інформації,
- конфіденційної інформації,
- інформації для службового користування.

Група пошуку і її оснащення

1. Формування групи пошуку (3-5 чоловік) для розв’язування завдань:

- проведення спеціальних перевірок об'єкта - виявлення природних і штучних каналів витоку інформації, а також локалізація технічних засобів перехоплення інформації на об'єкті;
- технічне обслуговування стаціонарних засобів захисту інформації, що установлені на об'єкті;
- видача рекомендацій з результатів спеціальної перевірки й за правилами експлуатації стаціонарних засобів захисту інформації.

2. Визначення регламенту різних видів спеціальних перевірок: разова, планово-профілактична, конспіративна.

3. Визначення рівнів "глибини перевірок":

- перший - виявлення радіовипромінювальних виробів, установлених безпосередньо в приміщеннях, що перевіряються, і суміжних з ними, а також телефонних передавачів, установлених на телефонних лініях, заведених у приміщення, що перевіряються;
- другий - виявлення всіх виробів першого рівня плюс мережеві передавачі, що використовуються для передачі інформації через мережу живлення 220В/50 Гц;
- третій - виявлення всіх виробів другого рівня плюс всі типи кабельних мікрофонів і систем, що передають акустичну інформацію приміщення по телефонних лініях, а також виявлення різних типів оргтехніки й сигналізації, що працює в режимі передачі корисної акустичної інформації за межі об'єкта охорони;
- четвертий - виявлення всіх типів закладних засобів перехоплення інформації, у тому числі й тих, що під час перевірки не працюють, а також можливі природні канали витоку інформації.

4. Оснащення групи пошуку. Звичайне оснащення групи включає у себе номенклатуру технічних засобів відповідного призначення, що наводиться нижче.

Пошукове обладнання:

- для перевірки радіоефіру;
- для оцінювання ефективності систем захисту;
- для керування сканерами й архівації результатів спецперевірок;

- для перевірки кабельних комунікацій на предмет виявлення сторонніх гальванічних підключень;
- для виявлення каналів витоку інформації й локалізації підслуховувальних пристроїв;
- для виявлення пасивних технічних засобів перехоплення інформації.

Допоміжна апаратура:

- комплект ультрафіолетових маркерів;
- ультрафіолетовий ліхтар;
- фотоапарат/відеокамера;
- комплект радіостанцій (3-4 шт.);
- цифровий мультиметр;
- диктофон і комплект касет;
- потужний ліхтар;
- трубка телефоніста;
- комплект оглядових дзеркал з підсвітчуванням;
- портативний металодетектор.

Сумісність системи ПЕШ із іншими системами

Можливість сумісності з діючими на об'єкті технологіями, зокрема, з роботою охоронної (охоронно-пожежної) сигналізації, системи охоронного відеоспостереження й системи контролю й керування доступом на об'єкті.

Додаткові вимоги

Додаткові вимоги до системи ПЕШ:

- технічні засоби активного зашумлення не повинні становити біологічну загрозу співробітникам і відвідувачам об'єкта інформатизації;
- усі технічні засоби, що використовуються для побудови системи захисту інформації, повинні мати сертифікати відповідності України.

Даний розділ пояснювальної записки повинен обов'язково містити:

- структурну (функціональну) схему розміщення обладнання системи ПЕШ;
- специфікацію (технічні характеристики) обладнання, що застосовується, й програмного забезпечення (у додатку);

− кошторис витрат для оснащення об'єкта захисту системою ПЕШ.

2.4.9 Комплекс захисту корпоративної мережі

У даному розділі пояснювальної записки повинні бути відображені короткі відомості про комплекс захисту корпоративної мережі.

Відомості про об'єкт захисту

1. Об'єкти, що підлягають оснащенню комплексом захисту корпоративної мережі (найменування, характеристика діяльності).

2. Проблеми, що розв'язуються комплексом захисту (як мінімум контроль несанкціонованого доступу. Загальні дані про функціонування інформаційної системи.

3. Порядок призначення прав доступу до критичних ресурсів.

4. Регламент резервування й відновлення критичної інформації.

5. Наявність відповідального адміністратора мережі (безпеки мережі).

6. Розташування критичної інформації.

7. Інформаційні потоки критичної інформації відносно робітників станцій, серверів, сегментів.

8. Наявність систем електронного документообігу.

9. Наявність критичних для підприємства процесів електронної обробки й передачі даних.

10. Можливість цілодобової роботи.

Інформація про топологію мережі, мережевих з'єднань і вузлів

1. Карта мережі, наприклад, для мережі до 50 користувачів може виглядати так:

- кількість і тип серверів (платформи, операційні системи, сервіси*): Widows NT standalone або primary/backup controller,* або *Novell Netware 4.1/4.11/5.0;*
- додатки: *MS SQL 6.5/7.0, MS Exchange or Eserv, Print server & File server*;
- кількість і тип робочих станцій (платформи, операційні системи, додатки, завдання, що виконуються): *Windows 2000/XP, Windows 2003/VISTA, Linux, Unix;*

– мережеві протоколи, що використовуються: *TC/IP, Netbios, IPX*.

2. Указати на схемі сегменти й способи їх з'єднання (маршрутизатори, хаби, мости та інше).

3. Указати варіант організації виходу в *Internet:*

– підключення виділеного комп'ютера (спосіб підключення, авторизації та ін.);
– підключення мережі (спосіб підключення, використання проксі-служб та інше);
– необхідність контролю трафіку й розмежування доступу користувачів;
– наявність усередині підприємства власного *WEB, FTP* серверів.

Використання вбудованих (придбаних) засобів моніторингу, безпеки й архівації

1. Захист персональних комп'ютерів від НСД (аудит, розмежування доступу), захист і розмежування доступу до персональних комп'ютерів при роботі на них декількох користувачів.

2. Міжмережеві екрани - захист від зовнішніх/внутрішніх атак.

3. Системи авторизації.

4. Антивірусний захист.

5. Засоби архівування, режим їхньої роботи.

6. Системи протоколювання дій користувачів.

7. Криптографічний захист.

8. Засоби системного аудиту.

9. Системи моніторингу мережі.

10. Захист обчислювальної техніки від злому, крадіжок.

11. Аналізатори протоколів.

12. Сканери - сканування ресурсів мережі на можливі поразки й видача рекомендацій для їх усунення.

13. Поділ критичних сегментів мережі.

14. Системи моніторингу безпеки - перевірка правильності настроювання корпоративних серверів, моніторинг безпеки корпоративної мережі в реальному часі.

Особливості функціонування комплексу

1. Можливості подальшого розширення шляхом додання до системи

пристроїв.

2. Необхідність і умови сумісності з існуючими системами (елементами) автоматизації обліку, технологічного процесу на об'єктах.

3. Необхідність і умови сумісності з існуючими системами (елементами) систем безпеки корпоративної мережі об'єкта.

4. Наявність сертифіката відповідності України на усе обладнання, що застосовується: класи захищеності АС, операційні системи, міжмережеві екрани, антивірусні засоби, рівень аналізу програмного забезпечення на недекларовані можливості.

Даний розділ пояснювальної записки повинен обов'язково містити:

- структурну (функціональна) схему мережі із вказанням елементів комплексу захисту;
- специфікації (технічні характеристики) устаткування й програмного забезпечення комплексу;
- кошторис оснащення об'єкта комплексом захисту корпоративної мережі.

2.4.10 Висновки

У висновках наводяться основні результати роботи над курсовим проектом. На основі проведених досліджень надається економічне обґрунтування проектів захисту (сумарний кошторис витрат по варіантах (не менш двох)) та обґрунтовані за критеріями показники захищеність/вартість, рекомендації для керівництва підприємства варіанти для впровадження на об'єкті захисту.

2.4.11 Література

Перелік містить список використаних джерел, які були застосовані в процесі виконання проекту, і на які повинні бути обов’язкові посилання в тексті пояснювальної записки. Література (книги, статті, патенти, журнали, інтернет-сторінки) в загальний список записується в порядку посилання на неї в тексті або у алфавітному порядку. Кожне джерело повинно бути вказано разом з видавництвом, роком видання, кількістю сторінок згідно з ДСТУ 7.1:2006 "Система стандартів з інформації, бібліотечної та ви-

давничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання". Літературу записують мовою оригіналу. У списку кожне джерело записують з абзацу, нумерують арабськими цифрами, починаючи з одиниці.

2.5 Додатки

Додатки повинні містити матеріал, який не увійшов в основні розділи пояснювальної записки: специфікації (основні технічні характеристики) пристроїв і систем, що використовуються; інформація про сертифікацію пристроїв і систем.

Кожен додаток необхідно починати з нової сторінки, вказуючи зверху посередині рядка слово “Додаток” і через пропуск – його позначення. Додатки позначають послідовно великими українськими буквами, за винятком букв Ґ, Є, З, І, Ї, Й, О, Ч, Ь, наприклад, Додаток А, Додаток Б і т.д. Якщо додатків більше ніж букв, то продовжують позначати арабськими цифрами. Дозволяється позначати додатки латинськими буквами, за винятком букв *I* і *O*.

Кожен додаток повинен мати тематичний (змістовний) заголовок, який записують посередині рядка малими літерами з першої великої.

Сторінки додатків нумеруються, продовжуючи загальну нумерацію у пояснювальній записці. Всі додатки включають у зміст, вказуючи номер, заголовок і сторінки, з яких вони починаються.

3 ГРАФІК ВИКОНАННЯ КУРСОВОГО ПРОЕКТУ І ПОРЯДОК ЙОГО ЗАХИСТУ

Рекомендується такий графік виконання курсового проекту, який враховує самостійну роботу студентів під час 2-го триместру (10 тижнів).

Зміст розділу	Термін виконання
Отримання завдання на курсовий проект, розробка і оформлення індивідуального завдання	1 тижд.
Опис об'єкта інформатизації, що захищається.	2 тижд.
Система контролю й керування доступом на об'єкт	3 тижд.
Система охоронного телебачення	4 тижд.
Система охоронно-пожежної сигналізації	5 тижд.
Протидія економічному шпигунству	6 тижд.
Комплекс захисту корпоративної мережі	7 тижд.
Оформлення пояснювальної записки до курсового проекту. Здача курсового проекту на попередню перевірку	8 тижд.
Корегування і доповнення пояснювальної записки та графічної документації згідно із зауваженнями керівника курсового проекту, врахування і виправлення пояснювальної записки	9 тижд.
Захист курсової роботи	10 тижд.

Готовність до захисту курсового проекту визначає керівник за результатами попередньої перевірки якості пояснювальної записки та графічної документації. Записка повинна бути здана керівнику на перевірку не менш, як за тиждень до визначеного терміну захисту проекту. Якщо проект виконаний в повному обсязі і не має принципових помилок, керівник допускає студента до захисту. В іншому випадку проект повертається студенту на доопрацювання. Після позитивного висновку про готовність курсового проекту студент повинен захистити її перед комісією у складі двох викладачів, які призначені кафедрою.

ПЕРЕЛІК ЛІТЕРАТУРИ

Основна

1. Алексеенко В. Н., Древс Ю. Г. Основы построения систем защиты производственных предприятий и банков. - М.: МИФИ, 1996. - 68 с.
2. Бармен С. Разработка правил информационной безопасности.: Пер. с англ. – Издательский дом «Вильямс», 2001. – 208 с.
3. Барсуков В. С., Водолазкий В. В. Современные технологии безопасности. М.: "Нолидж", 2000. – 496 с.
4. Блэк У. Интернет: протоколы безопасности. Учебный курс. – СПб.: Питер, 2001. – 288 с.
5. Волобуев С. В. Безопасность социотехнических систем. – Обнинск: "Викинг", 2000. – 340 с.
6. Гаценко О. Ю. Защита информации. Основы организационного управления. СПб.: Изд. дом "Сентябрь", 2001. – 228 с.
7. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Кн.1. – М.: Энергоиздат, 1994. - Кн.1 - 400 с. Кн.2. - 176 с
8. Герасименко В. А., Малюк А. А. Основы защиты информации. - М.: МИФИ, 1997. – 537 с.
9. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2005. – 144 с.
10. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – К.:ТИД "ДС", 2004. – 688 с.
11. Дудихин В. В., Дудихина О. В. Конкурентная разведка в Internet. Советы аналитика – М:. ДМК Пресс, 2002. – 192 с.
12. Завгородний В. И. Комплексная защита в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ, 2001. - 264 с.
13. Зима В. М. и др. Основы резервирования информации и архивации файловых данных в вычислительных системах: Учебн. пособие/ Зима В. М., Молдовян А. А., Молдовян Н. Л. – СПб.: ВИККА , 1998. – 186 с.
14. Зима В. М. и др. Резервирование системных данных компьютера и безопасная инсталляция программ: Учебн. пособие. СПб.: ВИККА, 1998. -– 213 с.

15. Комплексная безопасность объекта: от теории к практике / С. М. Доценко, В.Ф. Шпак. – СП: ООО «Издательство Полигон», 2000.- 130 с.
16. Костогрызов А. И., Петухов А. В., Щербина А. М. Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа. – М.: Вооружение. Политика. Конверсия,1994. - 278 с.
17. Кульба В. В., Волков А. Е., Климов А. А., Швецов А. Р. Анализ и синтез систем контроля и защиты данных с использованием сетей Петри. – Тольятти, 1998. – 228 с.
18. Курило А. П., Зефиров С. Л., Голованов В. Б. и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
19. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информатизации. Учеб.пособие для вузов – М.: Горячая линия – Телеком, 2004.- 280 с.
20. Мельников В. В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
21. Мельников В.В. Защита инофрмации в компьютерных системах. - М.: Финансы и статистика, 1997. – 364с.
22. Мишин Е. Т., Соколов Е. Е. Построение систем физической защиты потенциально опасных объектов. – М.: "Радио и связь", 2005. –200 с.
23. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия - Телеком. 2006. - 544 с: ил.
24. Петренко С. А., Петренко А. А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с.
25. Проскурин В. Г. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб.пособие для вузов /Проскурин В. Г., Крутов С. В., Мацкевич И. В. – М.: Радио и связь, 2000. – 168 с.
26. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.
27. Семененко В. А. Информационная безопасность. Учебное пособие. – М.: МГИУ, 2006. – 277 с.

28. Семкин С. Н., Беляков Э. В., Гребенев С. В., Козачок В. И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М.: Гелиос АРВ, 2005.– 192 с.
29. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.
30. Соколов А. В., Степанюк О. М. Методы информационной защиты объектов и компьютерных сетей. – М.: ООО "Фирма "Издательство АСТ"; – СПб: ООО "Издательство "Полигон", 2000. – 272 с.
31. Хоффман Л. Дж. Современные методы защиты информации. - М.: Советское радио, 1980. – 305 с.
32. Шумский А. А. Системный анализ в защите информации: учеб.пособие для студентов вузов, обучающихся по специальностям в обл.информ.безопасности / А. А. Шумский, А. А. Шелупанов. – М.: Гелиос АРВ, 2005.–224 с.

Додаткова

1. Захист інформації. Аналіз об’єкта// Бизнес и безопасность. – 2004.– №1. – С.41-42
2. Комплексные системы обеспечения безопасности торговых предприятий// Бизнес и безопасность. – 2004.– №3. – С.35-37
3. Комплесное обеспечение безопасности объектов КСБО_КМ// Бизнес и безопасность. – 2005.– №6. – С.22; – 2005.– №4. – С.28; – 2005.– №3. – С.36-37.
4. Методичні вказівки до оформлення курсових проектів (робіт) у Вінницькому національному технічному університеті /Уклад. Г. Л. Лисенко, А. Г. Буда, Р. Р. Обертюх. – Вінниця: ВНТУ, 2006. – 60 с.
5. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
6. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

7. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
8. Общие критерии безопасности информационных технологий. ISO/IEC 15408:1999. Information Technology. Security techniques. Evaluation criteria for IT security.
9. Основы информационной безопасности : курс лекций : учебное пособие / Издание третье / Галатенко В. А. Под редакцией академика РАН В. Б. Бетелина/ – М.: ИНТУИТРУ «Интернет-университет информационных технологий», 2006. – 208 с.
10. Плескач В. Л., Гладун А. Я. Проектування та створення комплексних систем захисту інформації для корпорацій // Бизнес и безопасность. – 2007.– №2. – С.98
11. Построение комплексных систем безопасности. Интеграция решений «BSI-Group» // Бизнес и безопасность. – 2006.– №5. – С.26-27
12. Практические правила управления информационной безопасностью. ISO/IEC 17799:2000. Information Technology. Code of practice for information security management.
13. Проектування комплексних систем захисту інформації: Методичні вказівки, завдання на контрольну та курсову роботи /Уклад.: В. С. Орленко, В. О. Хорошко, Д. В. Чирков. – К.:ДУІКТ, 2005. – 14с.
14. Техническая безопасность объектов предпринимательства. I том/ Сост. Дворский М. Н., Палатченко С. Н. – К.: "А-ДЕПТ", 2006. –304 с. ("Концепции безопасности")
15. Техническая безопасность объектов предпринимательства. II том/ Сост. Дворский М. Н., Палатченко С. Н. – К.: "А-ДЕПТ", 2006. –252 с. ("Концепции безопасности")
16. Технология безопасности промышленного предприятия. Интеграция решений на базе ИСПЕКТОР+ // Бизнес и безопасность. – 2004.– №2. – С.38-41

Додаток А

Приклад оформлення титульного аркуша

Міністерство освіти і науки України
Вінницький національний технічний університет
Інститут інформаційних технологій та комп'ютерної інженерії

Кафедра ОТ

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Пояснювальна записка
з дисципліни "Проектування комплексних систем захисту інформації"
до курсового проекту за спеціальністю 7.160104 – "Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом"
08-23.КСЗІ.007.13.000 ПЗ

Допущено до захисту:
_____ 200_ р. _____
(Дата) (Підпис керівника)

Керівник курсового проекту
к.т.н., ст.викл. каф. ОТ.
_____ Цирульник С. М.

Курсовий проект захищено
з оцінкою _____
_____ 200_ р. _____
(Дата) (Підпис керівника)

Розробив студент гр. АМЗ-04
_____Кузнецов Ю. В.

Вінниця ВНТУ 200_

Додаток Б

Приклад оформлення індивідуального завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Інститут інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ
Зав. кафедри ОТ, проф., д.т.н.
_____О.Д. Азаров
(підпис)
"___" _____ 200_ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

на курсовий проект
з дисципліни "Проектування комплексних систем захисту інформації "

студенту групи _____АМЗ04_____ факультету__КСМ_____ варіант К47
_____Кузнецову Юрію Володимировичу_____
(прізвище, ім'я, по батькові)
ТЕМА ___Розробка комплексної системи захисту об'єкта інформатизації_

Постановка задачі

Розробити проект комплексної системи захисту, що включає такі підсистеми:

- контролю і управління доступом на об'єкт;
- відеоспостереження (охоронного телебачення);
- охоронно-пожежну сигналізацію;
- протидії економічному шпигунству (аудіоінформація, некомп'ютерні канали зв'язку, паразитні електромагнітні випромінювання і наведення);
- захисту корпоративної мережі (внутрішньої та зовнішньої, електронний документообіг, антивірусний захист, міжмережеві екрани і інше).

Вихідні дані:

Категорія системи захисту інформації: *II*
Категорія об'єкта захисту: *C*

Характеристика об’єкта захисту: *Науково – дослідна лабораторія. 3-й поверх 4-поверхового цегляного будинку, який находиться на межі контрольованої зони*

Термін здачі студентом завершеного проекту_____

Зміст пояснювальної записки

Вступ

1. Опис об'єкта інформатизації, що захищається.
2. Політика інформаційної безпеки.
3. Перелік інформації, що складає комерційну таємницю.
4. Системи контролю і управління доступом на об'єкті.
5. Система охоронного телебачення.
6. Система охоронно-пожежної сигналізації.
7. Протидія економічному шпигунству.
8. Комплекс захисту корпоративної мережі.

Висновки

Література

Графічна частина:

- план об’єкта охорони;
- структурна (функціональна) схема розміщенням устаткування системи контролю і управління доступом на об'єкті;
- структурна (функціональна) схема розміщення відеокамер, устаткування системи й постів охорони системи охоронного телебачення;
- структурна схема системи захисту території об'єкта з розміщенням устаткування охоронно-пожежної сигналізації;
- структурна (функціональна) схема розміщення обладнання системи протидії економічному шпигунству;
- структурна (функціональна) схема мережі із вказанням елементів комплексу захисту корпоративної мережі.

Дата видачі ”____” _____ 200_ р. Керівник ____
(підпис)

Завдання отримав_____
(підпис)

Навчальне видання

Методичні вказівки до виконання курсового проекту з дисципліни «Проектування комплексних систем захисту інформації» для студентів спеціальності 7.160104 “Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом”

Укладач Сергій Михайлович Цирульник

Оригінал-макет підготовлено укладачем

Науково-методичний відділ ВНТУ
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ

Підписано до друку
Формат 29,7х42 1/4
Друк різографічний
Тираж прим.
Зам. №

Гарнітура Times New Roman
Папір офсетний
Ум. друк. арк.

Віддруковано в комп’ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ