ПРАКТИЧНА РОБОТА №5

СКЛАДАННЯ ІМОВІРНІСНОГО ПРОГНОЗУ ТА МОДЕЛІ ПОРУШНИКА

Мета – отримання практичних навичок складання ймовірнісного прогнозу; прогнозування та оцінка моделей порушника.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Оцінка можливостей порушника щодо подолання засобів захисту автоматизованих систем

Для проведення оцінки нам необхідно визначити компетентності порушника. В якості порушника розглядається суб'єкт, який має доступ до роботи зі штатними засобами інформаційно-телекомунікаційних систем (ІТС) і ПК як частини ІТС. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами ІТС, інформаційними систем (ІС). Класифікація є ієрархічною, тобто кожен наступний рівень включає в себе функціональні можливості попереднього.

Виділяється чотири рівні цих можливостей [1-4]:

Перший рівень визначає найнижчий рівень можливостей ведення діалогу в ІТС (ІС) - запуск програмного забезпечення та задач з визначеного набору, що реалізують, заздалегідь передбачені функції по обробці інформації відповідно до посадових функцій.

Другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації, що передбачені політикою безпеки підприємства (організації).

Третій рівень визначається можливістю управління функціонуванням ІТС (ІС), тобто з можливістю впливу на базове програмне забезпечення системи, її на склад, конфігурацію та устаткування.

Четвертий рівень визначається всім обсягом можливостей осіб, які здійснюють проектування, реалізацію та ремонт технічних засобів ІТС (ІС), аж до включення до складу ІТС власних технічних засобів з новими функціями з обробки інформації.

Вважаємо, що у своєму рівні порушник є фахівцем вищої кваліфікації, знає все про ІТС і, зокрема, про систему і засоби її захисту.

Крім рівня знань порушника, його кваліфікації, підготовленості до реалізації своїх задумів, для формування найбільш повної моделі порушника необхідно визначити категорію осіб, до яких може належати порушник.

В загальному випадку порушників можна розділити на **внутрішніх та зовнішніх**. Отримуємо наступні відкриті класифікаційні угрупування:

$\mathbf{N} = \bigcup_{\gamma} N_{\gamma}$ – множина персоналу, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність ІТС (ІС);

$\mathbf{Z} = \bigcup_{j} Z_j$ – множина потоку відвідувачів та контрагентів, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність ІТС (ІС)

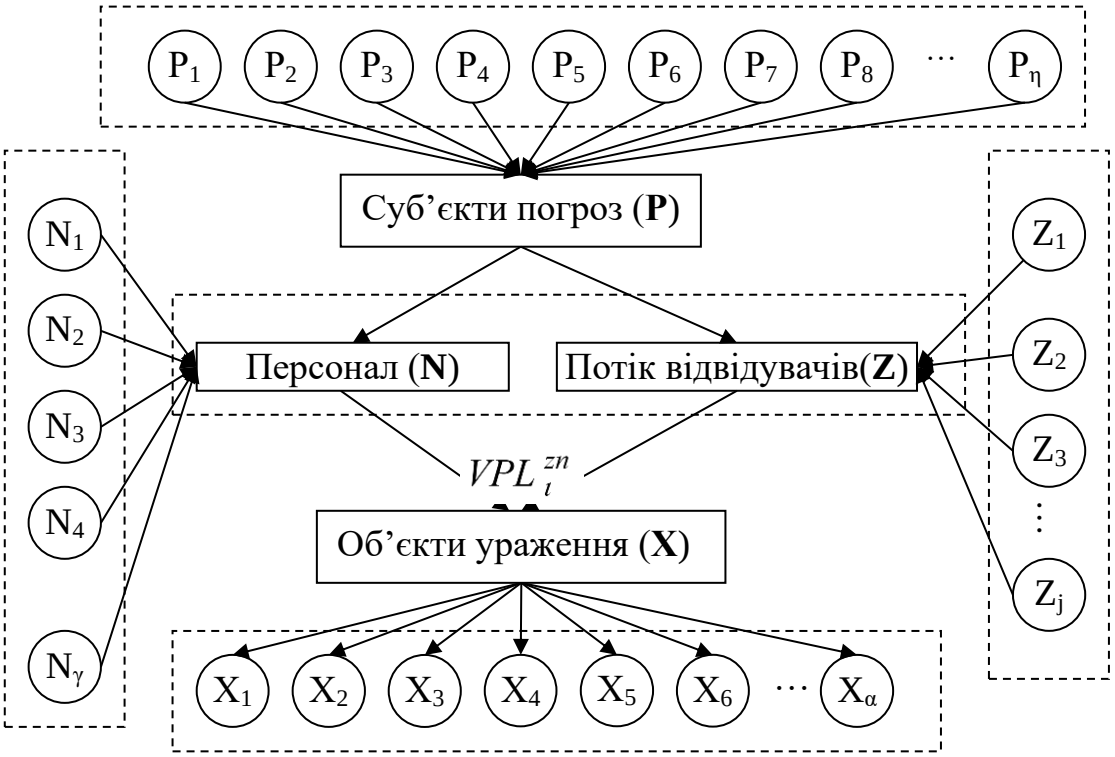

Рисунок 1.1. Модель прояву суб'єктів погроз виникнення НС на території аеропорту

Виходячи з рис. 1.1, маємо відкрите класифікаційне угрупування суб'єктів погроз, представлене у вигляді об'єднання множин потенційних учасників (реалізаторів) погроз виникнення загроз безпеки:

$$\mathbf{P} = \mathbf{N} \bigcup \mathbf{Z} = (N \setminus Z) \vee (Z \setminus N) \vee (Z \wedge N) \tag{1}$$

Таким чином, визначено джерела небезпеки у вигляді множини суб'єктів погроз (Р), які можуть реалізувати свої погрози через потік відвідувачів (клієнтів, контрагентів) (Z) або (та) персонал (N), які, в свою чергу, можуть здійснити дії (впливи) на об'єкти ураження та спровокувати виникнення загрози кібервтручання. Неважливо, чи є у вашої системи зв'язок із зовнішнім

світом, і чи є зовнішній захист, **але захист від внутрішніх порушників повинен бути обов'язково**.

Враховуючи той факт, що кожна організація має свою специфіку діяльності, не може існувати єдиної моделі порушника. Тому, при розробці заходів безпеки необхідно розглядати всі можливі для даної організації категорії порушників, яких можна класифікувати наступним чином, таблиця 1.1:

Таблиця 1.1. Класифікація порушників

Зовнішні порушники	**Внутрішні порушники**
Конкуренти	Системні адміністратори
Клієнти, контрагенти	Співробітники IT-відділу
Відвідувачі	Користувачі (оператори) системи
Хакери	Керівний склад організації
Злочинні організації	Технічний персонал
Звільнені співробітники	Співробітники служб безпеки

При створенні моделі порушника й оцінці ризику втрат від дій персоналу необхідно диференціювати всіх співробітників по їх можливостям доступу до системи і, отже, по потенційному збитку від кожної категорії користувачів. Наприклад, оператор або програміст ІС може завдати незрівнянно більший збиток, ніж звичайний користувач, тим більше непрофесіонал.

Таким чином, кожен користувач у відповідності зі своєю категорією ризику може завдати більший або менший збиток системі. Крім того, необхідно враховувати, що користувачі різних категорій розрізняються не тільки за ступенем ризику, а й по тому, якого елементу системи вони загрожують найбільше. В результаті можна *оцінити ступінь ризику даної категорії користувачів щодо даного елемента системи* і представити результати аналізу у вигляді таблиці відповідностей.

Одним з варіантів градації ризику може бути наступний [1,2]:

- Найбільший ризик - 5
- Підвищений ризик - 4
- Середній ризик - 3
- Обмежений ризик - 2
- Низький ризик - 1
- Немає загрози – 0

Нижче наводиться таблиця 1.2, в рядках якої перераховані що наведені вище категорії користувачів, а в стовпцях – найбільш вразливі елементи

системи. Таблиця показує, який ступінь ризику даної категорії користувачів щодо даного елемента систем.

Таблиця 1.2.Ступінь ризику для різних категорій користувачів

	Елементи АС																	
	I			**II**			**III**			**IV**			**V**			**VI**		
Види збитків / ***Категорії користувачів***	**A**	***B***	***C***	**A**	***B***	***C***	**A**	***B***	***C***	**A**	***B***	***C***	**A**	***B***	***C***	**A**	***B***	***C***
Інженер системних магнітних носіїв											4	4		3	3		3	3
Користувач-операціоніст	2	2	2		1	1				2	2	2		1	1			
Оператор системи	1	5	5		5	5		5	5	1	3	3						
Оператор периферійного обладнання											3	3		4	4		1	1
Оператор завдань											3	3		4	4			
Оператор вводу та підготовки даних	3	3	3		4	4		5	5	3	3	3		4	4		1	5
Менеджер обробки	1	5	5		5	5		5	5	1	3	3		4	4		1	5
Адміністратор баз даних	3	3	3							3	3	3						
Системний програміст		5	5		5	5	5	5	5							5	1	5
Прикладний програміст	1	1	1	2	2	2							2	2	2			
Користувач- програміст	1	1	1	2	2	2							2	2	2			
Менеджер програмного забезпечення	1	1	1	4	4	4							4	4	4			
Інженер/оператор по зв’язку		5	5															
Інженер системи							2	2	2									
Адміністратор безпеки	5	5	5	5	5	5	5	5	5	3	3	3	4	4	4	5	5	5
Системний адміністратор	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Уразливі компоненти системи:

I - внутрішні дані

II - внутрішні прикладні програми

III - внутрішні системні модулі

IV - зовнішні дані

V - зовнішні системні модулі

VI - елементи комп'ютера та ін апаратура.

Види загроз:

A - модифікація,

B - знищення,

C - компрометація (розкриття) інформації.

Як видно з таблиці, різні категорії користувачів можуть по-різному впливати на різні частини ІТС. Ці тонкощі корисно враховувати як при проектуванні системи, так і при її експлуатації.

Далі кожну групу ймовірних порушників необхідно проаналізувати окремо за наступними параметрами:

- Дані необхідні порушнику і період їх актуальності;
- Технічна оснащеність і використовувані для вчинення порушення методи та засоби;
- Передбачувані місця і час здійснення незаконних дій порушника;
- Обмеження і припущення про характер можливих дій;
- Кількісна оцінка часу, який порушник може витратити для подолання захисту (рисунок 1.2).

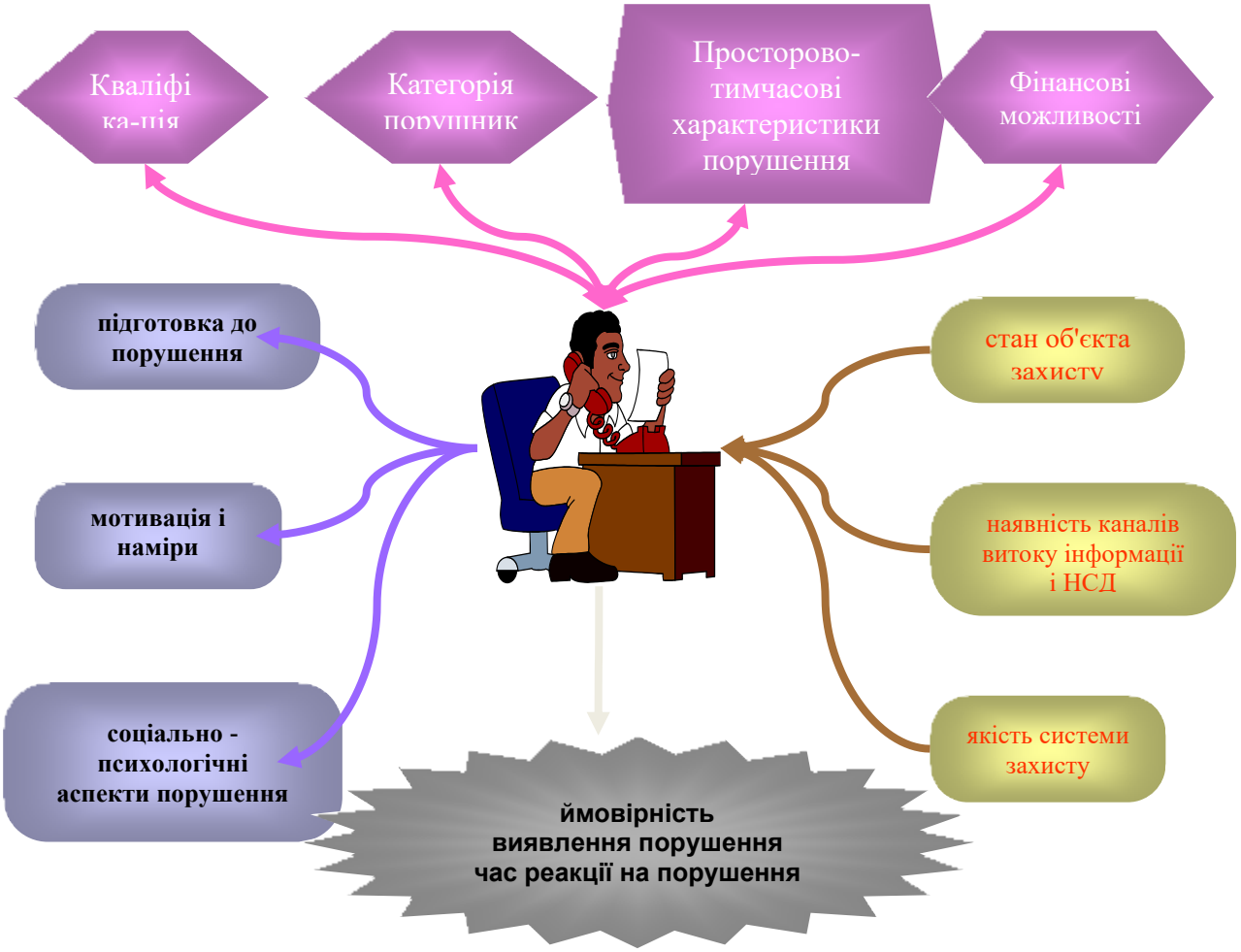

Рисунок 1.2. Схематична модель дій порушника

За технічної оснащеності та методами і засобами, що використовуються, порушники поділяються на тих, що:

- застосовують пасивні засоби (засоби перехоплення без модифікації компонентів системи);
- використовують тільки штатні засоби і недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів);

- застосовують методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

Наведена класифікація передбачає, перш за все, знання і постійне їх поповнення про характеристики технічних і програмних засобів ведення розвідки і забезпечення доступу до інформації.

Незаконні дії порушник може здійснювати:

- *В різний час* (в процесі функціонування ІС, під час роботи компонентів системи, під час планових перерв у роботі ІС, в неробочий час, в перерви для обслуговування і ремонту і т.п.);

- *З різних місць* (за меж контрольованої зони ІС; всередині контрольованої зони ІС, але без доступу в виділені для розміщення компонентів ІС приміщення; всередині виділених приміщень, але без доступу до технічних засобів ІС; з доступом до технічних засобів ІС і з робочих місць кінцевих користувачів; з доступом в зону даних, архівів тощо; з доступом в зону управління засобами забезпечення безпеки ІС).

Облік місця і часу дій зловмисника також дозволить конкретизувати його можливості по доступу до інформаційних ресурсів і врахувати їх для підвищення якості системи захисту інформації.

Визначення значень можливих характеристик порушників в значній мірі суб'єктивно. Модель порушника, побудована з урахуванням особливостей конкретної предметної області та технології обробки інформації, може бути представлена перерахуванням декількох варіантів його вигляду.

Для того, щоб розроблена модель порушника приносила користь у вирішенні проблем інформаційної безпеки, а не була простою формальністю, вона повинна бути строго адаптована до конкретного об'єкта інформаційної захисту. Крім того, кожен блок моделі порушника повинен мати продовження як у вигляді причинно-наслідкових зв'язків між окремими блоками, так і у вигляді деталізації інформації, що міститься в кожному блоці. Така деталізація передбачає побудову ланцюжків передбачуваних наслідків настання тих чи інших висновків щодо вигляду порушника.

Наявність сукупності моделей дій порушника може бути корисною з точки зору прогнозування можливих подій у всьому розмаїтті ситуацій, що складаються, запобігання дій порушника, побудови надійної системи захисту інформації, використання сучасних засобів інтелектуальної підтримки для управління системою захисту.

Серед обмеження і припущення про характер дій можливих порушників можуть бути наступні:

- робота з підбору кадрів та спеціальні заходи ускладнюють можливість створення коаліцій порушників, тобто об’єднання (змови) і цілеспрямованих дій щодо подолання підсистеми захисту двох і більше порушників;

- порушник, плануючи спроби НСД, приховує свої несанкціоновані дії від інших співробітників;

- НСД може бути наслідком помилок користувачів, адміністраторів, що експлуатує та обслуговуючого персоналу, а також недоліків прийнятої технології обробки інформації і т.д.

Один зі спрощених варіантів табличного оформлення моделі порушника наведено Таблиці 1.3-1.10. Для побудови даної моделі використовується 4-х бальна шкала оцінювання.

Таблиця 1.3. Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
	Внутрішні по відношенню до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Побудова причинно - наслідкових зв’язків між елементами моделі і ланцюжків передбачуваних наслідків вимагає знань в області соціально-психологічних аспектів діяльності порушника, в галузі техніки промислового шпигунства, можливостей засобів інформаційного захисту та цілого ряду інших, нерозривно пов'язаних з проблемою захисту інформації.

Таблиця 1.4. Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Таблиця 1.5. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 1.6. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 1.7. Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 1.8. Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Далі виводимо два варіанти сумарного рівня загроз для окремих категорій можливих порушників:

1) внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов'язків;

2) зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

Зведемо все у таблицю 1.9.

Таблиця 1.9. Сумарна рівень загроз дляокремих категорій порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
1	2	3	4	5	6	7	8
прибиральник	ПВ1	М1	К1	З1	Ч4	Д1	9
	1	1	1	1	4	1	
	ПЗ4	М4	К4	З4	Ч4	Д1	21
	4	4	4	4	4	1	
електрик	ПВ1	М1	К1	З1	Ч1	Д1	8
	1	1	1	1	3	1	
	ПЗ4	М4	К4	З4	Ч1	Д1	20
	4	4	4	4	3	1	
технік	ПВ2	М1	К2	З1	Ч4	Д3	12
	2	1	2	1	4	2	
	ПЗ4	М4	К4	З4	Ч4	Д3	22
	4	4	4	4	4	2	
юрист	ПВ3	М1	К2	З1	Ч3	Д2	11
	2	1	2	1	3	2	
	ПЗ4	М4	К4	З4	Ч3	Д2	21
	4	4	4	4	3	2	
адміністратор	ПВ4	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К4	З4	Ч4	Д4	24
	4	4	4	4	4	4	

1	2	3	4	5	6	7	8
працівник служби безпеки	ПВ5	М1	К1	З1	Ч4	Д3	14
	4	1	1	1	4	3	
	П34	М4	К4	З4	Ч4	Д3	23
	4	4	4	4	4	3	

Після зведення усіх даних 1-го варіанту в одну таблицю отримаємо таку табличну «Модель внутрішнього порушника політики безпеки інформації», таблиця 1.10.

Таблиця 1.10. Модель внутрішнього порушника політики безпеки інформації

Категорія порушника «ПВ»	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Служба безпеки	М1	К1	З1	Ч4	Д3	14
Адміністратор ІТС	М1	К4	З1	Ч4	Д4	17
Користувач	М1	К2	З1	Ч3	Д2	11
Технік ІТС	М1	К2	З1	Ч4	Д3	12
Електрик	М1	К1	З1	Ч1	Д1	8
Прибиральник	М1	К1	З1	Ч4	Д1	9

Аналіз останньої таблиці показує, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС. Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

Таким чином представлено побудову моделі порушника та досліджено її особливості формування.

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Провести вибір об’єкту захисту та представити короткий опис діяльності.
3. Визначити організаційну структуру об’єкту дослідження та представити її у звіті.
4. Провести оцінку ступеня ризику для різних категорій користувачів відносно елементу системи відповідно до таблиці 1.2.
5. Побудувати модель порушника відповідно до наведених таблиць 1.3-1.10 для вибраного об’єкту дослідження.
6. Зробити висновки та оформити звіт.

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть основні типи та мотивацію порушень концепції безпеки підприємства.
2. Які категорії порушників Ви знаєте?
3. Назвіть типи конфліктів, які можуть виникати в організації?
4. Назвіть категорії порушників, які є потенційно небезпечними.
5. Назвіть основні заходи та методи захисту інформації від НСД.
6. Яким чином, на вашу думку, можна заохотити персонал до якісного виконання професійних обов’язків?
7. Якою є мотивація до роботи для Вас особисто?
8. Які наслідки можуть бути від розголошення інформації для організації?
9. Які наслідки розголошення інформації можуть бути для працівника?
10. Перерахуйте засоби та технології захисту інформації в кібернетичному просторі, які Ви знаєте?