Лабораторна робота №6

ДОСЛІДЖЕННЯ ПРОЦЕСІВ СКЛАДАННЯ ІМОВІРНІСНОГО ПРОГНОЗУ ТА МОДЕЛІ ПОРУШНИКА

Мета – дослідження процесів несанкціонованого доступу до інформації; дослідження процесів складання ймовірнісного прогнозу; дослідження процесів прогнозування та оцінка моделей порушника.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Оцінка можливостей порушника щодо подолання засобів захисту автоматизованих систем

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, автоматизованих систем (АС). Класифікація є ієрархічною, тобто кожен наступний рівень включає в себе функціональні можливості попереднього.

Виділяється чотири рівні цих можливостей.

Перший рівень визначає найнижчий рівень можливостей ведення діалогу в ІТС (АС) - запуск задач (програм) з фіксованого набору, що реалізують, заздалегідь передбачені функції по обробці інформації.

Другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації.

Третій рівень визначається можливістю управління функціонуванням ІТС (АС), тобто впливом на базове програмне забезпечення системи, і на склад, і на конфігурацію її устаткування.

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

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.

У загальному випадку всі порушники можуть бути внутрішніми (з числа персоналу) або зовнішніми (сторонніми особами). Результати досліджень причин порушень (за даними Datapro Information Services Group та інших організацій) говорять про одне: головне джерело порушень – усередині самої автоматизованої системи: 75-85% порушень здійснюються самими службовцями організації, що мають доступ до її системи, і лише 15-25% порушень здійснюються особами з боку. І висновок звідси також однозначний: 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:

Таблиця1 – Класифікація порушників

Зовнішні порушники	Внутрішні порушники
Конкуренти	Адміністратори
Клієнти (представники сторонніх організацій, громадяни)	Співробітники відділів розробки і супроводу ПЗ (прикладні та системні програмісти)
Відвідувачі	Користувачі (оператори) системи
Хакери	Керівники різних рівнів посадової ієрархії
Злочинні організації	Технічний персонал

Вона повинна використовуватися для визначення можливостей щодо незаконного доступу до інформації, що циркулює в ІТС.

1.1. Конкуренти

Зазначений вид порушника є найнебезпечнішим, оскільки володіє найбільшими фінансовими можливостями і кваліфікацією. Об'єктом нападу в першу чергу є комерційна таємниця об'єкта і клієнтів. Зазначений вид порушника є найбільш агресивним і небезпечним, оскільки володіє значним техніко-економічним потенціалом і буде намагатися отримати потрібну йому інформацію всіма можливими способами: шляхом злому автоматизованої банківської системи, підкупу співробітників об'єкта і т.п. Порушників даного типу досить складно виявити, оскільки збитки від витоку інформації може бути неявним, цілі порушника можуть бути розраховані на далеку перспективу.

1.2. Клієнти

Зазначений вид порушника є далеко не найпоширенішим, і мало значним. Метою атак даного типу порушників може бути система електронних платежів. Атаки робляться з метою відмови від авторства платіжного документа, або твердження про формування неіснуючого платіжного документа.

1.3. Відвідувачі

Відвідувачів можна розділити на клієнтів об'єкта та інших відвідувачів. Відвідувачі, знаходячись на території об'єкта, можуть мати за мету:

- отримувати доступ до персональних комп'ютерів;
- ставати свідком конфіденційних переговорів між співробітниками об'єкта;
- отримати доступ до інформації будь-якого роду на паперових носіях;
- отримувати доступ до інформаційних каналах і встаткування.

Інші відвідувачі Об'єкту слід віднести до нечисленної і безпечною категорії порушників. Їх метою є одержання, в процесі переговорів зі співробітниками Об'єкта і, на підставі, почутих розмов, інформації закритого характеру, або використання можливості проникнення на закриту територію для проведення диверсій.

1.4. Хакери

Зазначена група порушників є самою нечисленною групою, але, зважаючи на їх високої кваліфікації, несе потенційну небезпеку. Слід зазначити, що в разі їх взаємодії з конкурентами і внутрішніми порушниками хакери є найбільш небезпечними зловмисниками, оскільки можуть, отримавши інформацію про внутрішню структуру мережі і проходять по ній інформаційних потоках, створити ситуації, що перешкоджають функціонуванню мережі. Зокрема:

- зупинка, збій серверів;
- несанкціонований доступ до інформації;

- знищення та / або модифікацію програмного забезпечення;
- створення множинних неправдивих інформаційних повідомлень, що призводять до перевантаження серверів і інформаційних каналів і як наслідку – відмова в обслуговуванні користувачів системи.

1.5. Адміністратори

Зазначена група потенційних порушників мережі є досить небезпечною групою серед внутрішніх порушників, не дивлячись на свою нечисленність. Через їх високої кваліфікації та специфіки виконання завдань. Зокрема, ними можуть бути відтворені всі ситуації, що перешкоджають функціонуванню мережі (зупинка, збій серверів; знищення та / або модифікацію програмного забезпечення, створення множинних, помилкових інформаційних повідомлень). Крім того, йому доступний несанкціонований знімання інформації, блокування роботи окремих користувачів, перебудова планів маршрутизації і політик доступу мережі.

1.6. Програмісти

Зазначена група потенційних порушників, з причини своєї високої кваліфікації прав в програмних комплексах несе в собі завуальовані і важко розпізнавані загрози, зокрема:

- в разі доступу до реальних баз даних: може вносити неконтрольовані зміни в розроблюваний програмний продукт і в бази даних;
- вбудовувати в розроблювані продукти: системи несанкціонованого доступу; системи блокування роботи по умовному ключу або команді.

1.7. Оператори

Зазначена група потенційних порушників, незважаючи на свою численність і можливість доступу до баз даних, не є високо критичною. Оскільки, при правильній організації роботи, всі їхні дії протоколюються, і вони мають доступ тільки до незначної частини інформації.

1.8. Керівники

Зазначена група ймовірних порушників, потенційно є дуже небезпечною в першу чергу через великі прав доступу в банківську систему. А саме: у зв'язку з повноваженнями, даними їм, як керівникам, мають безпосередньо доступ до перегляду та зміни критичної інформації, і видозміні її при змові. Друге, звичайно не ведуть належного обліку використання своїх прав доступу в систему, в першу чергу не дотримуються рекомендованих рамок при зміні пароля, що може дозволити сторонньому користувачеві, підібравши пароль, зробити будь-які дії від його особи.

1.9. Технічний персонал

Іінженери і техніки, обслуговуючі технічні засоби, будівлі мають доступ в приміщення, виділені для розміщення компонентів ІТС).

Зазначена група порушників володіє специфічними можливостями по створення незареєстрованих точок входу і виходу з локальної мережі, створення незареєстрованих вузлів мережі, зміна топології мережі і т.п.

1.10. Співробітники, звільнені з роботи

Зазначена група може володіти специфічними можливостями, які в першу чергу залежать від колишніх прав порушника при роботі в системі. З найбільш часто зустрічаючих ситуацій слід відзначити продаж конкурентам інформації про внутрішню організації справ, розпорядок діловодства. У разі якщо звільнений технічний співробітник: інформації про топологію мережі, своїх імен і паролів у системі.

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 автоматизованої банківської системи 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:

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

Нижче наводиться таблиця 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 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***
Бібліотекар системних магнітних носіїв											4	4		3	3		3	3
Бібліотекар магнітних носіїв користувачів											2	2		1	1			
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 обработки	1	5	5		5	5		5	5	1	3	3		4	4		1	5
Адміністратор баз данных	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 контролер	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.

Безумовно, як відомості з таблиці, так і наведені вище категорії персоналу системи за ступенем ризику не слід сприймати як догму. Просто при аналізі власних ІТС *складіть подібну таблицю* для полегшення всієї подальшої роботи.

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).

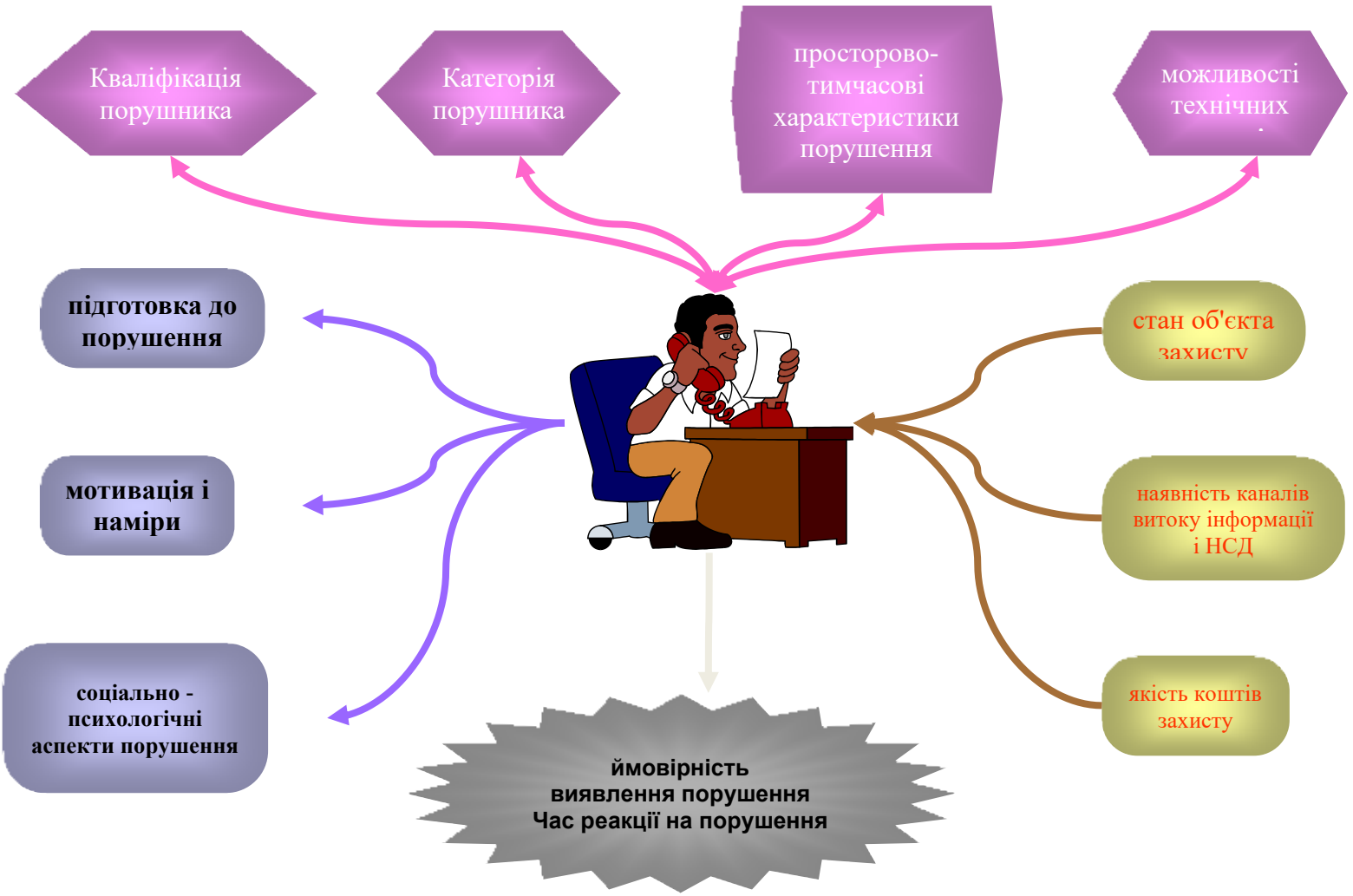

Рисунок 1

За технічної оснащеності і використовуваним методам і засобам порушники поділяються на:

- 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 АС, під час роботи компонентів системи, під час планових перерв у роботі АС, в неробочий час, в перерви для обслуговування і ремонту і т.п.);

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

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.

Для того, щоб розроблена модель порушника приносила користь у вирішенні проблем інформаційної безпеки, а не була простою формальністю, вона повинна бути строго адаптована на конкретний об'єкт інформаційного захисту. Крім того, кожен елемент моделі порушника повинен мати продовження як у вигляді причинно-наслідкових зв'язків між

окремими елементами, так і у вигляді деталізації інформації, що міститься в кожному з них. Така деталізація передбачає побудову ланцюжків передбачуваних наслідків настання тих чи інших висновків щодо вигляду порушника. Один зі спрощених варіантів табличного оформлення моделі порушника наведено у Додатку 1.

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.

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Провести оцінку порушників по визначенню засобів захисту автоматизованих систем або ІТС підприємства.
3. Провести оцінку ступеня ризику для різних категорій користувачів відносно елементу системи.
4. Побудувати модель порушника відповідно до наведеної таблиці.
5. Зробити висновки та оформити звіт.

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть основні типи та мотивація 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.

ЗМІСТ ЗВІТУ.

1. Назва, мета й завдання.
2. Опис дій в ході виконання завдання.
3. Висновки про виконане завдання.

Додаток 1

Тип впливу	Тип порушника	Місце виникнення	Час виявлення	Місця системи, що піддаються атаці	Ймовірність		Доведеність
					Виникнення	Своєчасне виявлення	
Протиправне вилучення або переведення фінансових засобів	ОП	Робоче місце користувача	По факту, при проведенні перевірки	ПК	3	1	4
				БП; БК	3	1	6
	АДМ	Всередині системи		БП	0	2	1
				БК, ПК	0	6	0
	ПРОГ			БП; БК; ПК	0	5	1
	РУК			БП; БК; ПК	0	2	6
	ТЕХ			БП; ПК	-	0	-
				БК	0	3	0
	ХАК	Всередині системи		ПК	5	3	5
				БП	-	0	-
				БК	0	5	3
		Зовні системи		БП; ПК	-	0	-
			В момент перевірки цифрового підпису	БК	6	2	6
	ВНЕШ			БК	6	1	6
Необережні дії, що призводять до розголошення конфіденційної інформації	АДМ	Всередині системи	По факту, при проведенні перевірки	СЕРВ; БД	0	6	2
	ПРОГ			БД	0	5	0
	ХАК			СЕРВ	0	4	3
				БД	0	1	4

ОП – оператори;
АДМ – адміністратори;
ПРОГ – програмісти;
РУК – керівники;
ТЕХ – технічний персонал;
ХАК – хакери;
ВНЕШ – зовнішні порушники;

ПК – платіжна система пластикових карт;
БК – система платежів банк-кліент;
БД – любі бази данних з інформацією про діяльність об’єкту

СЕРВ – сервера;
СЕТЬ – працездатність мережевого обладнання та пропускна здатність мережі;
КомП – компьютери користувачів;
БП – система платежів;

Дія, що призводить до часткової або повної відмови системи	АДМ	Робоче місце	По факту події	СЕРВ	0	5	2
		Поза системою		БД	0	2	3
	ПРОГ	Робоче місце		СЕРВ	0	3	2
				БД	0	6	0
	ХАК	Всередині системи		СЕРВ	2	4	5
				БД	1	3	5
				СЕТЬ	3	5	5
		Ззовні системи		СЕРВ	6	1	6
				ПК	5	4	5
				БД	-	0	-
				СЕТЬ	6	1	6
Неправомірна зміна топології мережі	АДМ	Внутрішні системи	По факту здійснення атаки	СЕТЬ	0	6	0
	ПРОГ				0	5	0
Неправомірне відключення обладнання або зміна режимів роботи	АДМ	Внутрішні приміщення	По факту здійснення	СЕТЬ	0	6	2
				Сеть 220	0	6	1
	ПРОГ			СЕТЬ,Сеть220	0	4	2
	ВНЕШ			СЕТЬ	0	1	3
				Сеть220	0	2	4
	ТЕХ			СЕТЬ	1	6	1
				Сеть220	1	6	2
	РУК			Сеть220	1	6	3
Псування носіїв інформації . Управління інформаційними технологіями	АДМ	Робоче місце	По факту здійснення	Місце збереження резервних копій	0	6	4
	ПРОГ	Внутрішні приміщення			0	3	4
	ВНЕШ				0	1	5
	ТЕХ				0	3	4
Псування носіїв інформації	АДМ	Робоче місце	По факту здійснення	Місце збереження резервних копій	0	6	0
	ПРОГ	Внутрішні приміщення			0	3	0