МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист інформації в спеціалізованих ІТС

Практичне заняття №1

Дослідження сучасних трендів захисту інформації в спеціалізованих ІКС

Перевірив:
Зубок В. Ю.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2025

Завдання (Варіант №10: Парний)**:** За матеріалами ПРАВИЛ системи електронних платежів Національного банку України, а також ПОЛОЖЕННЯ про використання засобів криптографічного захисту інформації проаналізувати організаційно-технічні вимоги, яким мають задовольняти учасники системи електронних платежів (СЕП).

1. Скільки модулів генерації ключів отримує учасник системи?

За положенням про використання засобів криптографічного захисту інформації НБУ, організаціям надається модуль генерації ключів (МГК) у двох екземплярах – основний та резервний. Тобто учасник системи отримує **два модулі генерації ключів**.

2. Які основні вимоги до розташування та використання апаратури засобів захисту інформації, отриманих від НБУ?

Основні вимоги, що стосуються апаратури можна сформулювати наступним чином:

- **Безпечне розміщення**. Обладнання повинно бути встановлено в окремих, спеціально обладнаних приміщеннях із забезпеченням фізичної безпеки (обмежений доступ, опечатування приміщення, відеоспостереження, контроль входу тощо).

- **Використання згідно з нормативними вимогами**. Експлуатація апаратури має здійснюватися виключно згідно з встановленими інструкціями та нормативними документами НБУ, що гарантують належний рівень захисту інформації.

- **Відповідність адресі розташування**. Обладнання не можна встановлювати за адресою, відмінною від тієї, яка вказана в укладених договорах (н/д, у Єдиному договорі банківського обслуговування); будь-які зміни місцезнаходження мають бути негайно доведені до відома НБУ.

3. Які ролі щодо використання АРМ МГК мають бути в організації?

Для належного використання АРМ МГК (інформаційної системи для управління ключовими даними засобів генерації ключів) організація має визначити такі ролі:

- **Відповідальна особа (оператор АРМ МГК).**

Ця особа безпосередньо проводить генерацію ключової пари за допомогою АРМ МГК і відповідає за захист свого особистого ключа (використання паролю). Генерація ключів має здійснюватися згідно з експлуатаційною документацією та встановленими процедурами.

- **Адміністратор інформаційної безпеки.**

Він (або вони) відповідає за організаційне, технічне та процедурне забезпечення експлуатації АРМ МГК, контроль доступу до засобів криптографічного захисту та своєчасне оновлення/обслуговування апаратури. Також адміністратор контролює дотримання внутрішніх нормативних актів щодо використання засобів КЗІ.

- **Керівництво організації.**

Затверджує політику використання криптографічних засобів, у тому числі АРМ МГК, забезпечує необхідні ресурси та організаційну підтримку, а також визначає повноваження та відповідальність відповідних співробітників.