МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МЕТОДИЧНІ ВКАЗІВКИ

до самостійної роботи з дисципліни

“СТЕГАНОГРАФІЧНІ СИСТЕМИ”

для студентів усіх форм навчання
спеціальності 125 «Кібербезпека»,
спеціалізації «Безпека інформаційних і комунікаційних систем»

Електронне видання

ЗАТВЕРДЖЕНО
кафедрою БІТ
Протокол № 1 від 29.08.2017

ХАРКІВ 2017

Методичні вказівки до самостійної роботи з дисципліни “Стеганографічні системи ”. Для студентів усіх форм навчання спеціальності 125 «Кібербезпека», спеціалізація «Безпека інформаційних і комунікаційних систем»[Електронне видання] /Упорядник О.І. Федюшин. - Харків: ХНУРЕ, 2017. - 19 с.

Упорядник О.І. Федюшин

Рецензент О.Качко, професор каф. ПЗЕОМ

ЗМІСТ

ВСТУП

Дисципліна «Стеганографічні системи» присвячена вивченню основ стеганографічного захисту інформації, методів та обчислювальних алгоритмів стеганографічного перетворення, дослідження відповідних атак на стеганосистеми та вивчення методів протидії.

1. ЦІЛЬ ТА ЗАДАЧІ ДИСЦИПЛІНИ

Предметом вивчення навчальної дисципліни є процеси, механізми, методи, системи та засоби стеганографічного захисту інформації в інформаційних системах (ІС) та інформаційно-телекомунікаційних системах (ІТС).

Програма навчальної дисципліни складається з таких розділів:

1. Вступ до цифрової стеганографії;
2. Стеганографічні методи приховування даних в контейнерах-зображеннях;
3. Стеганографічні методи приховування даних в аудіофайлах
4. Лінгвістична та технічна стеганографія.

Метою викладання навчальної дисципліни є формування у студентів певних професійних компетенцій, знань та вмінь у галузі цифрової стеганографії, методів та обчислювальних алгоритмів приховування факту існування інформації та створення водяних знаків.

Основними *завданнями* з вивчення навчальної дисципліни є отримання студентами необхідних базових знань з теоретичних основ побудови стеганографічних систем захисту інформації, моделей та методів стеганографічного перетворення та обчислювальних алгоритмів приховування факту існування інформації та створення водяних знаків.

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких *результатів навчання*:

ЗНАТИ:

- визначення, класифікацію та основні властивості стеганографічних систем;

- математичні моделі стеганографічних перетворень та абстрактне визначення стеганографічних систем;
- методи та обчислювальні алгоритми стеганографічного захисту інформації при вбудовуванні даних в графічні зображення, аудіосигнали, текстові документи;
- визначення, класифікацію та основні атаки на стеганосистеми та методи протидії;

ВМІТИ:

- практично реалізовувати обчислювальні алгоритми стеганографічного перетворення, зокрема, алгоритми приховування та вилучення даних із графічних зображень, аудіосигналів, текстових документів;
- оцінювати пропускну спроможність каналів передавання схованої інформації, рівень внесених похибок в контейнери-оригінали та ймовірнісні властивості стеганографічних систем (ймовірність помилкового вилучення інформаційних повідомлень, тощо);
- оцінювати стійкість стенографічних систем до різних атак на стеганографічні системи.

Сфера реалізації набутих компетенцій в майбутній професії.

В межах професійної діяльності вміти розробляти вимоги та обирати для застосування стеганосистеми та стеганопротоколи, що мінімізують впливи порушників; вибирати та застосовувати критерії та показники оцінки стійкості стеганосистем та безпечності стеганопротоколів; обґрунтовувати вимоги до ключових систем та управління ключовими даними стеганосистем, здійснювати аналіз їх властивостей; проводити аналіз та синтез стегано-протоколів за критерієм безпечності, порівнювати їх з використанням умовних та безумовних критеріїв; застосовувати стандартні пакети при розв’язанні прикладних задач моделювання стеганосистем, ключових систем і стеганографічних протоколів. Тобто показати здатність використовувати інструментальні засоби і системи програмування для вирішення професійних завдань; здатність до програмної реалізації алгоритмів розв'язання типових задач забезпечення інформаційної безпеки.

2. РОБОЧА ПРОГРАМА ДИСЦИПЛІНИ

При вивченні дисципліни використовуються знання та практичні навички, що отримані під час вивчення шкільного курсу з предмету «Інформатика»,

отриманих в процесі вивчення дисциплін підготовки бакалаврів напряму «Кібербезпека»: «Інформаційно-комунікаційні системи», «Інформаційні технології», «Технології програмування», «Прикладна криптологія».

Навчальна програма дисципліни містить два модуля та чотири змістовних модуля.

Перша частина дисципліни «Стеганографічні системи» присвячена питанням визначення, класифікації та опису основних властивостей стеганографічних систем; а друга частина дисципліни – вивченню стеганографічних методів приховування даних, а також розгляду математичних моделей стеганографічних перетворень

Структура дисципліни:

МОДУЛЬ1.Стеганографічні системи.

Змістовний модуль 1. Вступ до стеганографії

Тема 1. Цифрова стеганографія. Предмет, термінологія, галузь використання

1. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами навчального плану

2. Цифрова стеганографія. Предмет, термінологія, галузь використання

Тема 2. Математична модель та структурна схема стеганосистеми

1. Структурна схема та формальне математичне визначення криптографічної (секретної) системи. Ймовірності показники та умова теоретично недешифрованої секретної системи.

2. Математична модель та структурна схема стеганографічної системи. Ймовірності показники та умова теоретично недетектованої стеганографічної системи.

Тема 3. Атаки на стегосистеми

1. Класифікація атак на секретні та стеганографічні системи

2. Атаки на системи прихованої передачі повідомлень та на системи цифрових водяних знаків (ЦВЗ).

МОДУЛЬ2. Стеганографічні методи приховування даних

Змістовний модуль 2. Стеганографічні методи приховування даних в контейнерах-зображеннях

Тема 4. Особливості зорової системи людини (ЗСЛ), які використовуються в стеганографії. Основні формати цифрових зображень

1. Особливості ЗСЛ, які використовуються в стеганографії
2. Основні формати цифрових зображень. Растрові дані. Формат зображень Bitmap Picture (bmp)

Тема 5. Приховування даних у просторовій області нерухомих зображень

1. Методи приховування на основі модифікації найменш значущого біту даних (НЗБ)
2. Блокове приховування, метод квантування, метод «хреста»

Тема 6. Приховування даних із використанням технології прямого розширення спектру

1. Складні дискретні сигнали та технологія прямого розширення спектру
2. Приховування даних із застосуванням складних дискретних сигналів

Тема 7. Приховування даних у частотній області нерухомих зображень

1. Основні етапи алгоритму стиску зображень JPEG. Дискретно-косинусне перетворення
2. Метод Коха-Жао та його модифікації
3. Метод Фридріх

Змістовний модуль 3. Стеганографічні методи приховування даних в аудіофайлах

Тема 8. Особливості слухової системи людини (ССЛ), які використовуються в стеганографії. Основні формати аудіофайлів

1. Особливості ССЛ та їх застосування в стеганографії
2. Основні формати аудіофайлів. Формат аудіофайлів Waveform Audio Format (wav)

Тема 9. Приховування даних у просторовій області аудіо сигналів

1. Методи приховування на основі модифікації НЗБ

2. Метод кодування луна-сигналів

Тема 10. Приховування даних у частотній області аудіо сигналів

1. Основні властивості дискретного перетворення Фурье. Амплітудний, частотний та фазові спектри аудіосигналів

2. Метод фазового кодування

Змістовний модуль 4. Лінгвістична та технічна стеганографія

Тема 11. Приховування даних у текстових документах

1. Лінгвістичні властивості, які використовуються в стеганографії

2. Методи приховування даних на основі довільних інтервалів

3. Синтаксичні методи приховування даних

4. Семантичні методи приховування даних

Тема 12. Стеганографічні методи із застосуванням технологій 3D друку

1. Класифікація та основні властивості відомих технологій 3D друку

2. Штучна надмірність 3D моделей, яка використовується в стеганографії

3. Методи приховування даних із застосуванням технологій 3D друку

Тема 13. Приховування даних у кластерних файлових системах

1. Особливості побудови файлових систем зберігання даних

2. Штучна надмірність кластерних файлових систем, яка використовується в стеганографії

3. Методи приховування даних у кластерних файлових системах

Тема 14. Мережева стеганографія

1. Методи модифікації вмісту інформаційних пакетів

2. Методи модифікації полів заголовків телекомунікаційних протоколів

3. Гібридні методи

Навчальний час вивчення дисципліни розподіляється наступним чином:

лекції	– 24
практичні заняття	–4
лобораторні роботи	–20
консультації -	–8

самостійна робота –64
усього годин –120

2.1 Лекційні заняття

Лекції є основним видом навчальних занять на яких вивчаються найбільш важкі теоретичні питання дисципліни, а також питання оглядового характеру, орієнтуючи студентів на подальшу самостійну роботу з рекомендованою літературою. Дисципліна передбачає модульний (блоковий) метод засвоєння. Матеріал розділений на чотири змістовних модулі, після завершення яких передбачається виконання контрольних робіт, або тестування.

Розподіл тем за змістовними модулями, видами занять і структура залікових кредитів наведені в таблиці 2.1. Перелік тематичних розділів лекційних занять у цій таблиці згрупований у двогодинні лекції. До цих же тематичних розділів приєднані і теми практичних занять. Обсяг часу, запланований для самостійної роботи над лекційним матеріалом і виконанням домашніх індивідуальних занять, зазначений в окремому стовпчику.

Таблиця 2.1 – Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
МОДУЛЬ 1.Стеганографічні системи												
Змістовний модуль 1. Вступ до стеганографії												
Тема 1. Цифрова стеганографія. Предмет, термінологія, галузь використання	4	2				2						
Тема 2. Математична модель та структурна схема стеганосистеми. Критерії та показники ефективності	10	2	2			6						

стеганосистем												
Тема 3. Атаки на стегосистеми	4	2				2						
Разом за розділом 1	18	6	2			10						
МОДУЛЬ 2. Стеганографічні методи приховування даних												
Змістовний модуль 2. Стеганографічні методи приховування даних в контейнерах-зображеннях												
Тема 4. Особливості ЗСЛ, які використовуються в стеганографії. Основні формати цифрових зображень	4	2				2						
Тема 5. Приховування даних у просторовій області нерухомих зображень	12	2		8		2						
Тема 6. Приховування даних із використанням технології прямого розширення спектру	10	2		4		4						
Тема 7. Приховування даних у частотній області нерухомих зображень	8	2		4		2						
Разом за розділом 2	34	8	0	16		10						
Змістовний модуль 3. Стеганографічні методи приховування даних в аудіофайлах												
Тема 8. Особливості ССЛ, які використовуються в стеганографії. Основні формати аудіофайлів	6	2				4						
Тема 9. Приховування	11	1		2		8						

даних у просторовій області аудіо сигналів												
Тема 10. Приховування даних у частотній області аудіо сигналів	11	1		2		8						
Разом за розділом 3	28	4	0	4		20						
Змістовний модуль 4. Лінгвістична та технічна стеганографія												
Тема 11. Приховування даних у текстових документах	9	1	2			6						
Тема 12. Стеганографічні методи із застосуванням технологій 3D друку	7	1				6						
Тема 13. Приховування даних у кластерних файлових системах	8	2				6						
Тема 14. Мережева стеганографія	8	2				6						
Разом за розділом 4	32	6	2			24						
Консультації за розкладом	8											
Усього годин	144	24	4	20		64						

2.2 Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми (форма поточного контролю)	Кількість годин
1	Математична модель та структурна схема стеганосистеми. Критерії та показники ефективності стеганосистем. (ПЗ1)	2
2	Приховування даних у просторовій області нерухомих зображень. Методи приховування на основі модифікації НЗБ (ЛР1)	4

3	Приховування даних у просторовій області нерухомих зображень. Блокове приховування, метод квантування, метод «хреста» (ЛР2)	4
5	Приховування даних із застосуванням складних дискретних сигналів та технології прямого розширення спектру (ЛР3)	4
6	Приховування даних у частотній області нерухомих зображень. Метод Коха-Жао та його модифікації (ЛР4)	4
7	Стеганографічні методи приховування даних в аудіофайлах (ЛР5)	4
8	Приховування даних у текстових документах (ПЗ2)	2
	Разом	24

2.3 Самостійна робота

№ з/п	Назва теми	Кількість годин	Форма контролю
1	Цифрова стеганографія. Предмет, термінологія, галузь використання	2	Поточний контроль у формі усного опитування
2	Математична модель та структурна схема стеганосистеми (КР1)	6	Поточний контроль у формі усного опитування
3	Атаки на стегосистеми	2	Поточний контроль у формі усного опитування
4	Особливості зорової системи людини (ЗСЛ), які використовуються в стеганографії. Основні формати цифрових зображень	2	Поточний контроль у формі усного опитування
5	Приховування даних у просторовій області нерухомих зображень(КР2)	2	Поточний контроль у формі усного опитування
6	Приховування даних із використанням технології прямого розширення спектру(КР3)	4	Поточний контроль у формі усного опитування
7	Приховування даних у частотній області нерухомих зображень(КР4)	2	Поточний контроль у формі усного опитування
8	Особливості ССЛ, які використовуються в стеганографії. Основні формати аудіофайлів	4	Поточний контроль у формі усного опитування
9	Приховування даних у просторовій області аудіо сигналів(КР5)	8	Поточний контроль у формі усного опитування
10	Приховування даних у частотній області аудіо сигналів	8	Поточний контроль у формі усного опитування
11	Приховування даних у текстових	6	Поточний контроль у

	документах (КР6)		формі усного опитування
12	Стеганографічні методи із застосуванням технологій 3D друку	6	Поточний контроль у формі усного опитування
13	Приховування даних у кластерних файлових системах	6	Поточний контроль у формі усного опитування
14	Мережева стеганографія(КР7)	6	Поточний контроль у формі усного опитування
	Разом	64	

Індивідуальні завдання

Індивідуальні завдання студентів пов'язані з вивченням окремих, в тому іноземних джерел, за тематикою дисципліни, проведенням аналізу існуючих та перспективних засобів захисту інформації, дослідженням рівнів стійкості, розробленням імітаційних моделей та дослідженням ефективності в тому числі із застосуванням принципу масштабування. Теми індивідуальних завдань, як правило, пов'язуються з науковими та науково - методичними дослідженнями, які веде кафедра та інші підрозділи університету чи інші підприємства чи заклади тощо, фірми.

Основними формами реалізації результатів виконання індивідуального завдання є:

– доповідь чи виступ на семінарських чи практичних заняттях;

– доповідь на тематичних науково - практичних конференціях з опублікуванням тез чи доповідей;

– підготовка та опублікування наукових та науково - практичних статей;

– підготовка та подання результатів досліджень для використання в НДР та ДКР кафедри;

– участь в розробці науково - методичних та навчальних матеріалів;

– підготовка патентів на винаходи та корисні моделі;

– розробка та опис програмних продуктів та моделей тощо.

2.4 Рекомендована література

Базова література

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2012 р., 878 с.

2. Есин В. И., Кузнєцов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.

3. Кузнецов О.О. Семенов С.Г. Протоколи захисту інформації у комп'ютерних системах та мережах. Х.:ХНУРЕ, 2009р. – 184.

4. Грибунин В.Г., Оков И. Н., Туринцев И. В.. Цифровая стеганография. Серия: Аспекты защиты. – Солон-Пресс, 2002 г. – 272 с.

5. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. МК-Пресс, 2006г. – 288 с.

6. Simmons G.J. The prisoner`s problem and the subliminal channel, Proc. Workshop on Communications Security (Crypto`83), 1984, 51-67.

7. Pfitzmann B. Information Hiding Terminology, in Information Hiding, Springer Lecture Notes in Computer Science, v.1174, 1996, 347-350.

8. Aura T. Invisible communication. In Proc. of the HUT Seminar on Network Security '95, Espoo, Finland, November 1995. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology.

9. Ross J. Anderson. Stretching the limits of steganography. In IH96 [3], pages 39-48.

10. Zollner J., Federrath H.,Klimant H., Pfitzmann A., Piotraschke R., Westfeld A., Wicke G., Wolf G. Modeling the security of steganographic system, Proc. 2nd International Workshop on Information Hiding, 1998, LNCS, v.1525, 344-354.

11. E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand. Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, In Information hiding: first international workshop, Cambridge, UK. Lecture Notes in Computer Science, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996.

Допоміжна література

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.

2. N.F. Johnson, S. Jajodia. Exploring Steganography: Seeing the Unseen, IEEE Computer, February 1998, vol. 31, no. 2, pp.26-34.

3. Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. IBM Systems Journal, 35(3 & 4):313{336, 1996.

4. Raymond B. Wolfgang and Edward J. Delp. A watermark for digital images. In International Conference on Images Processing, pages 219-222, Lausanne, Switzer-land, September 1996. IEEE.

5. Kahn D. The Codebreakers. N-Y, 1967.

6. Жельников В. Криптография от папируса до компьютера. М., 1996.

7. Радіотехніка. Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000 – 2015 рр.

8. Прикладная радиоелектроника. Научн. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематические выпуски «Безопасность информации» 2006 – 2015 рр.

Інформаційні ресурси

1. www.nist.gov
2. www.eprint.iacr.org
3. www.citeseer.ist.psu.edu
4. www.springerlink.com
5. www.cacr.math.uwaterloo.ca
6. www.financialcryptography.com
7. www.austinlinks.com
8. www.world.std.com/~franl/crypto.html
9. www.cryptonessie.org
10. www.osti.gov/eprints

3. ХАРАКТЕРИСТИКА ПІДРУЧНИКІВ І НАВЧАЛЬНИХ ПОСІБНИКІВ

Перелік наведених літературних джерел поділено на основні та додаткові. Підручники доступні в бібліотеці університету, а також електронних ресурсах кафедри БІТ.

Як базове джерело інформації рекомендовано використовувати електронний варіант конспекту лекцій з дисципліни, а також додатково методичні вказівки з практичних занять, лабораторних робіт, з самостійної роботи, які є в електронному вигляді. Вказані у додатковій літературі джерела доступні в обмеженій кількості в бібліотеці.

4 ЗАГАЛЬНІ МЕТОДИЧНІ ВКАЗІВКИ З ВИВЧЕННЯ ДИСЦИПЛІНИ

Самостійна робота є основним засобом оволодіння навчальним матеріалом у час, вільний від навчальних занять за розкладом. Вона проводиться з метою:

відпрацювання та засвоєння навчального матеріалу, закріплення та поглиблення знань, умінь та навичок, які одержані на всіх видах навчальних занять; виконання навчальних завдань та розв’язання задач; підготовки до

майбутніх занять та іспиту; формування у студента самостійності та ініціативи у пошуку та набутті знань.

Самостійна робота студентів активізує розумову діяльність, стимулює потребу в поглибленні одержаних знань шляхом використання різних видів самостійної роботи.

За характером організації всі види самостійної роботи можна поділити на дві групи: види самостійної роботи в процесі проведення очних занять і види самостійної роботи, що проводяться у позаурочний час.

Види організації самостійної роботи у процесі проведення очних занять.

Лекційні заняття.

Однією з форм організації самостійної роботи, що присутня на лекціях, є конспектування.

Добрий конспект лекцій – показник активної роботи студента на лекції, уміння творчо сприймати ним зміст програмного матеріалу.

Змістовне конспектування мотивує необхідність глибокого вивчення навчальної літератури, дозволяє зробити самостійну роботу цілеспрямованою.

Лабораторні заняття.

До числа найбільш ефективних методів активізації самостійної роботи студентів належать: імітаційний ігровий метод, метод ігрового виробничого планування, метод аналізу конкретних ситуацій, метод евристичного аналізу, дослідний метод, метод "мозкового штурму".

На лабораторних заняттях з дисципліни "Технології програмування" частіше за все використовуються дослідний метод та метод "мозкового штурму".

Дослідний метод полягає в розв’язанні проблемних, нестандартних задач, які поставлені викладачем.

Суть "мозкового штурму" – створення спеціальної групи студентів – генераторів ідей. Вони знаходять варіанти рішень задач і пропонують їх на загальне обговорення з наступним колективним аналізом.

Експеримент, як різновид дослідного методу, використовується в лабораторних роботах. Його використовують до вивчення теорії, що ставить студента в ситуацію "першовідкривача".

Види організації самостійної роботи, що виконуються студентами у позаурочний час:

До таких видів можна віднести:

- роботу з навчальною літературою, рекомендованою викладачем;
- робота з додатковою літературою, самостійно обраною студентом;
- підготовка до лабораторних занять;
- підготовка до атестаційного контролю;
- підготовка до здачі екзамену;
- виконання завдань в системі дистанційної освіти;

Загальна трудомісткість самостійної роботи складає 64 години (дивіться графік організації самостійної роботи нижче).

Види організації самостійної роботи, що можуть виконуватись студентами у режимі дистанційної освіти:

- робота з навчальною літературою;
- робота з конспектами лекцій;
- підготовка до лабораторних занять;
- виконання домашніх завдань та тестування.

Розподіл часу самостійної роботи для підготовки до різних видів занять, витрати часу на засвоєння лекційного матеріалу та рекомендованої літератури, витрати часу на виконання контрольних робіт наводиться в табл. 4.1

Таблиця 4.1– Розподіл часу самостійної роботи

№	Назва теми	Кількість годин	
		денна	заочна
1	Вивчення теоретичного матеріалу з використанням конспектів і навчальної літератури	16	
2	Підготовка до лабораторних занять	26	
3	Підготовка до практичних занять	12	
4	Підготовка до контрольних робіт	10	
Загальна кількість		64	

Методичні вказівки до самостійної роботи

1. Проробити використовуючи рекомендовану літературу і засвоїти за лекційним матеріалом зміст поточної теми робочої програми. Для перевірки ступеня засвоєння матеріалу скористатися наведеними за кожною темою контрольними запитаннями й оцінити свою готовність дати на них відповіді.

2. Під час підготовки до практичного заняття переглянути відповідний розділ методичних вказівок до практичних занять, у якому стисло викладено основні теоретичні положення теми, що виноситься на практичне заняття, а також ознайомитися з наведеними прикладами вирішення домашніх і аудиторних завдань і задач. Переглянути свої майбутні домашні завдання і задачі та підготувати для випадків, що викликають ускладнення, питання для обговорення на практичному занятті.

3. Під час підготовки до лабораторного заняття переглянути відповідний розділ методичних вказівок до лабораторних робіт, у якому стисло викладено основні теоретичні положення теми, зміст, мету та завдання, порядок виконання, що виноситься на лабораторну роботу, та питання до лабораторної роботи.

Електронний навчальний документ

МЕТОДИЧНІ ВКАЗІВКИ
до самостійної роботи

з дисципліни
СТЕГАНОГРАФІЧНІ СИСТЕМИ

для студентів усіх форм навчання
спеціальності 125 Кібербезпека
Освітня програма
"Безпека інформаційних та комунікаційних систем”

Упорядник Федюшин Олександр Іванович

Відповідальний випусковий Г.З. Халімов

Авторська редакція