

**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**

**ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ  
ІМЕНІ ГЕРОЇВ КРУТ**

## **НАВЧАЛЬНА ПЛАН-ПРОГРАМА**

**курсів підвищення кваліфікації  
з питань кібербезпеки**

**Київ – 2021**

## МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЗАТВЕРДЖУЮ  
Командувач Військ зв'язку та кібербезпеки  
Збройних Сил України  
генерал-майор

Євген СТЕПАНЕНКО

“03” 2021 року

## НАВЧАЛЬНА ПЛАН-ПРОГРАМА

курсів підвищення кваліфікації з питань кібербезпеки

**Категорія тих, хто навчається:** офіцери та персонал структурних підрозділів Міністерства оборони України, Генерального штабу Збройних Сил України та органів військового управління, військових частин та установ Збройних Сил України, військовослужбовці (призначені або зараховані до резерву кандидатів для просування по службі на відповідні посади), державні службовці категорії «В», які входять до складу служб захисту інформації та кібернетичної безпеки в ІТС, а також особи діяльність яких пов'язана з забезпеченням та організацією захисту інформації в захищеній системі електронного документообігу

**АРКУШ ПОГОДЖЕННЯ**  
**навчальної план-програми курсів підвищення кваліфікації з питань кібербезпеки**

**ПОГОДЖЕНО**

Директор Департаменту військової освіти і науки,  
Міністерства оборони України

  
“ 03 ” 01 2021 року

Володимир МІРНЕНКО

**ПОГОДЖЕНО**

Начальник Головного управління доктрин та  
підготовки Генерального штабу Збройних Сил України  
генерал-майор

  
“ 03 ” 01 2021 року

Олексій ТАРАН

**РОЗРОБЛЕНО І ВНЕСЕНО**

**Керівник закладу-розробника**

Начальник Військового інституту телекомунікацій та  
інформатизації імені Героїв Крут  
генерал-майор

  
“ 03 ” 01 2021 року

Віктор ОСТАПЧУК

## I. ЦІЛЬОВА НАСТАНОВА

Метою навчання на курсах підвищення кваліфікації з питань кібербезпеки офіцерів та персоналу структурних підрозділів Міністерства оборони України, Генерального штабу Збройних Сил України та органів військового управління, військових частин та установ Збройних Сил України, військовослужбовців (призначених або зарахованих до резерву кандидатів для просування по службі на відповідні посади), державних службовців категорії «В», які входять до складу служб захисту інформації та кібернетичної безпеки в ІТС, а також особи діяльність яких пов'язана з забезпеченням та організацією захисту інформації в захищеній системі електронного документообігу є набуття спеціальних та технічних знань, практичних навичок щодо контролю та забезпечення захисту інформації та кібербезпеки в частинах та підрозділах ЗС України.

## II. ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ ВКАЗІВКИ

Навчальна план-програма включає в себе: цільову настанову; організаційно-методичні вказівки; зведені дані з бюджету часу на навчальний курс (у годинах); за модулями, темами та видами навчальних занять; формами поточного та підсумкового контролю; інформаційно-методичного забезпечення.

План-програма складається з одного змістового модулю.

Комплексність навчання досягається викладанням теоретичного матеріалу відповідно до навчальної план-програми, отримання необхідних практичних навичок, складання заліку.

Перед початком навчання проводиться вхідний контроль з метою визначення рівня особистої підготовленості офіцерів.

Всього на навчання відведено 112 години протягом 2 тижнів, з них:

а) під керівництвом викладача виділяється 72 години, з них 36 годин теоретичний курс, практичний курс – 36 годин.

б) на самостійну підготовку слухачів виділяється 40 годин.

в) перевірка успішності та особистої підготовки слухачів проводиться під час проведення контролю та складання слухачами екзамену за змістовими модулями навчальної план-програми в кінці терміну навчання – 6 годин.

Навчання здійснюється шляхом проведення лекційних, групових, практичних занять, а також самостійної роботи слухачів з навчальним матеріалом.

Згідно з вимогами план програми забезпечується набуття **компетентності**:

знати основні принципи функціонування систем захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних мережах Збройних Сил України;

знати керівні документи з перевірки та експлуатації систем захисту інформації та управління елементами системи кібернетичної безпеки;

знати способи та засоби контролю та виконання вимог щодо захисту інформації на ОІД, інструкції та керівні документи з антивірусного захисту та протидії кібернетичним інцидентам.

знати вимоги та порядок створення комплексних систем захисту інформації;

Згідно з вимогами план програми визначені та сформульовані наступні **результати навчання**:

здійснювати організацію технічного захисту інформації у підрозділі;

здійснювати роботи по підготовці та експлуатації програмних та апаратних засобів в складі комплексних систем захисту інформації;

здійснювати заходи захисту інформації на об'єктах інформаційної діяльності в телекомунікаційних системах спеціального призначення.

**У змістовому модулі “Захист інформації та кібербезпека”** викладаються: основи технічного захисту інформації на об'єктах інформаційної діяльності; призначення, ТТХ основних зразків виявлення закладних пристроїв, способи виявлення та протидії ним. Способи криптографічного захисту інформації та види криптоперетворень. Способи та засоби кібернетичного захисту, протидії кібернетичним вторгненням, порядок налаштування та використання міжмережевих екранів, засобів антивірусного захисту. Методи та способи контролю та забезпечення безпеки інформації в ІТС ЗС України.

Активними формами навчання під час засвоєння навчальної програми є практичні заняття з використанням засобів ТЗІ, засобів криптографічного захисту інформації, засобів забезпечення кібербезпеки.

Інтенсифікація навчання і розвиток творчих здібностей досягається шляхом створення на заняттях нестандартної обстановки й відтворення проблемних ситуацій, відпрацюванням ситуаційних задач.

Практична підготовка забезпечується проведенням практичних занять.

Перевірка успішності і якості підготовки слухачів здійснюється у ході підсумкового контролю.

**III. ЗВЕДЕНІ ДАНІ З БЮДЖЕТУ ЧАСУ НА НАВЧАЛЬНИЙ КУРС  
(у годинах)**

Термін навчання	Всього годин	З них		Види занять				Звітність
		Аудиторних	Самостійні заняття	Лекції	Семінарські заняття	Групові заняття	Практичні заняття	
2 тижні	112	72	40	4		32	36	Екзамен

**IV. РОЗПОДІЛ НАВЧАЛЬНОГО ЧАСУ ЗА МОДУЛЯМИ  
ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ**

№ з/п	Назва кафедри	Назва модулю	Всього годин	З них		Аудиторні заняття				
				Аудиторні	Самостійні заняття	Лекції	Групові заняття	Семінарські заняття	Практичні заняття	Звітність (екзамен)
1.	Кафедра № 33	Захист інформації та кібербезпека	106	66	40	4	26		36	
		Екзамен	6	6			6			Екзамен
<b>Всього годин</b>			<b>112</b>	<b>72</b>	<b>40</b>	<b>4</b>	<b>32</b>		<b>36</b>	

**V. ТЕМАТИЧНИЙ ПЛАН ТА РОЗПОДІЛ НАВЧАЛЬНОГО ЧАСУ ЗА КАФЕДРАМИ, МОДУЛЯМИ,  
ТЕМАМИ, ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ**

№ з/п	Назва кафедри	Назва змістових модулів; шифр умінь, номери та назва тем і занять, їх зміст	Загальний обсяг годин	Аудиторних					Самостійна робота	Матеріально- технічне та інформаційне забезпечення
				Всього	за видами занять					
					Лекції	Семінарські заняття	Групові заняття	Практичні заняття		
1	2	3	4	5	6	7	8	9	10	11
<p align="center">Навчальні заняття містять інформацію з обмеженим доступом згідно наказу Генерального Штабу ЗС України №408 від 22.11.2017 року “Про затвердження Переліку відомостей ЗС України, що становлять службову інформацію”</p>										

## VI. ФОРМИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Вхідний контроль проводиться на першому занятті курсів у формі тестування.

Підсумковий контроль здійснюється шляхом складання екзамену за всією план-програмою наприкінці навчання.

Слухачі після закінчення курсів перепідготовки та підвищення кваліфікації отримують свідоцтво про закінчення курсів.

## VII. ІНФОРМАЦІЙНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

### Змістовий модуль № 1. Захист інформації та кібербезпека

1. Мазулевський О. Є., Самойлов І. В., Шевченко А. С. Захист інформації в телекомунікаційних системах і мережах Частина I / – К.: ВІТІ, 2015. – 258 с.
2. Хорев А.А. Способы и средства защиты информации. – М.: МО РФ, 2000. – 316 с.
3. Хорев П.Б. Методы и средства защиты информации в компьютерных сетях. – М.: Издательский центр "Академия", 2008. – 256 с.
4. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с., ил.
5. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность. – 344 с., ил.
6. Хорев А.А. Защиты информации от утечки по техническим каналам. – М., 1998. – 193 с.
7. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
8. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
9. НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
10. НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
11. Антонюк А.А. Захист інформації в автоматизованих системах.



12. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М: "Радио и связь", 2001. – 376 с.
13. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – ДМК Пресс, 2002. – 656 с.
14. Столингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: – М.: Издательский дом "Вильямс", 2001. – 672 с.
15. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.
16. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 368 с.
17. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. – Харків: видавництво «Форт», 2012. – 880 с.
18. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів: Бак, 2003. – 144 с.
19. Поповский В.В. Основы криптографической защиты информации в телекоммуникационных системах. Ч. 1./В.В. Поповский, А.В. Персиков. – Х.: «Компания СМИТ», 2010. – 352 с.
20. Поповский В.В. Основы криптографической защиты информации в телекоммуникационных системах. Ч. 2./В.В. Поповский, А.В. Персиков. – Х.: «Компания СМИТ», 2010. – 564 с.

Начальник кафедри Захисту інформації та кіберзахисту, доктор технічних наук, старший науковий співробітник  
полковник



Владислав ЧЕВАРДІН