МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
ІМЕНІ ГЕРОЇВ КРУТ

НАВЧАЛЬНА ПЛАН-ПРОГРАМА

курсів підвищення кваліфікації
з питань технічного захисту інформації

Київ – 2021

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЗАТВЕРДЖУЮ
Командувач Військ зв'язку та кібербезпеки Збройних Сил України
генерал-майор
Євген СТЕПАНЕНКО
"___" _____ 2021 року

НАВЧАЛЬНА ПЛАН-ПРОГРАМА

курсів підвищення кваліфікації з питань технічного захисту інформації

Категорія тих, хто навчається: офіцери, працівники Збройних Сил України та державні службовці Міністерства Оборони України, які виконують функції експертів у сфері технічного захисту інформації

АРКУШ ПОГОДЖЕННЯ

навчальної план-програми курсів підвищення кваліфікації з питань технічного захисту інформації

ПОГОДЖЕНО

Директор Департаменту військової освіти і науки, Міністерства оборони України

Володимир МІРНЕНКО

“ 03 ” 01 2021 року

ПОГОДЖЕНО

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

Олексій ТАРАН

“ 03 ” 01 2021 року

РОЗРОБЛЕНО І ВНЕСЕНО

Керівник закладу-розробника

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

Віктор ОСТАПЧУК

“ 03 ” 01 2021 року

І. ЦІЛЬОВА НАСТАНОВА

Підготовка на курсах підвищення кваліфікації офіцерів та працівників Збройних Сил України та державних службовців Міністерства Оборони України (військовослужбовці, державні службовці третьої-сьомої категорій та особи, призначені (зараховані до кадрового резерву для призначення) на відповідні посади) здійснюється з метою забезпечення та організації технічного захисту інформації у сфері відкритої інформації.

ІІ. ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ ВКАЗІВКИ

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

План-програма складається з одного модуля.

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

Всього на навчання відведено 40 годин протягом 1-го тижня, з них:

а) під керівництвом викладача виділяється 32 години, з них 20 годин теоретичний курс, практичний курс 12 годин. За розкладом занять на перший змістовий модуль відводиться – 40 годин навчальних занять.

б) на самостійну підготовку слухачів виділяється усього 8 годин.

в) перевірка успішності та особистої підготовки слухачів проводиться під час складання слухачами заліку в кінці терміну навчання – 2 години.

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 вимоги нормативно-правової бази з технічного захисту інформації в України;

знати основні вимоги Інструкція з організації антивірусного захисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України (Наказ МО України № 391);

знати основні вимоги Порядку використання мережі Інтернет у системі Міністерства оборони України (Наказ МО України №727);

знати вимоги та порядок створення комплексних систем захисту інформації;

знати порядок створення та документального оформлення моделі загроз, плану захисту інформації, технічного завдання на КСЗІ;

знати особливості захисту інформації в інформаційно-телекомунікаційних мережах;

знати порядок ведення експлуатаційної документації (журналів приймання-здавання чергування, технічних журналів тощо);

знати основні функції та призначення службу захисту інформації в ІТС.

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

здійснювати організацію технічного захисту інформації у підрозділі;

здійснювати розроблення моделі загроз, плану захисту інформації, технічного завдання на КСЗІ;

забезпечувати забезпечення антивірусного захисту в інформаційно-телекомунікаційних системах;

забезпечувати документальне супроводження на етапах створення КСЗІ.

У змістовому модулі " Забезпечення технічного захисту відкритої інформації, що є власністю держави, у Збройних Силах України " викладаються: основні засади організації технічного захисту інформації в Україні; класифікація інформаційно-телекомунікаційних систем: АС класу 1, АС класу 2, АС класу 3 (НД ТЗІ 2.5-005-99); забезпечення захисту інформації в ІТС; ДСТУ 3396.0-96 – „Технічний захист інформації. Основні положення"; ДСТУ 3396.1-96 – „Технічний захист інформації. Порядок проведення робіт"; загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1- 002-99); положення про службу захисту інформації (НД ТЗІ 1.4-001-00); порядок проведення робіт із створення КТЗІ в ІТС (НД ТЗІ 3.7-003-05); здійснюється практичне відпрацювання: моделі загроз, плану захисту інформації, технічного завдання на КСЗІ; Інструкція з організації антивірусного захисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України (Наказ МО України № 391); порядок використання мережі Інтернет у системі Міністерства оборони України (Наказ МО України №727).

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

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

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

Підсумковий контроль здійснюється на заліку за питаннями згідно навчальної план-програми наприкінці періоду навчання.

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

Термін навчання	Всього годин	З них		Види занять				
		Аудиторних	Самостійні заняття	Лекції	Семінарські заняття	Групові заняття	Практичні заняття	Звітність
1 тиждень	40	32	8	6		14	12	залік

ІV. 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	Забезпечення технічного захисту відкритої інформації, що є власністю держави, у Збройних Силах України	38	30	8	6	12		12	
		Залік	2	2			2			Залік
Всього годин			**40**	**32**	**8**	**6**	**14**		**12**	

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
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”										

VI. ФОРМИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Після повного виконання план-програми, з метою встановлення фактичної відповідності рівня підготовки слухачів курсів, проводиться підсумковий контроль у вигляді заліку.

VII. ІНФОРМАЦІЙНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Змістовий модуль № 1. Розробка комплексних систем захисту інформації

1. Мазулевський О. Є., Самойлов І. В., Шевченко А. С. Захист інформації в телекомунікаційних системах і мережах. Частина І / – К. : ВІТІ, 2015. – 258 с.
2. Закон України "Про інформацію".
3. Закон України "Про державну таємницю".
4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
5. Закон України "Про захист персональних даних".
6. Грайворонский М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. - Київ. видавнича група BHV, 2009. – 607 с.
7. Наказ Міністра оборони України № 106 від 04.03.2010 р. Порядок проведення державної експертизи в сфері технічного захисту інформації у Міністерстві оборони України та Збройних Силах України.
8. Наказ Міністерства оборони України від 26 листопада 2017 року № 391 "Про затвердження Інструкції з організації антивірусного захисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України".
9. Наказ Міністерства оборони України від 28 грудня 2016 року № 727 "Про затвердження Порядку використання мережі Інтернет у системі Міністерства оборони України".
10. Наказ Міністра оборони України від 01 жовтня 2011 року № 597 (зі змінами, внесеними наказом Міністерства оборони України від 30 жовтня 2015 року № 603) "Про затвердження Порядку використання автоматизованої системи управління Збройних Сил України "Дніпро".
11. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

12. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

13. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

14. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

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

полковник В. ЧЕВАРДІН