МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
імені ГЕРОЇВ КРУТ

НАВЧАЛЬНИЙ ПЛАН-ПРОГРАМА

курсу підвищення кваліфікації з питань підготовки особового складу штатних підрозділів – служб захисту інформації в автоматизованих системах
(ПСЗІАС–ТР)

Київ
2024

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
імені ГЕРОЇВ КРУТ

ЗАТВЕРДЖУЮ
Тимчасово виконуючий обв'язки начальника Головного Управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України – начальника зв'язку та кібербезпеки Збройних Сил України
полковник

Віталій ЖУКОВ

"___" _____ 2024 року

НАВЧАЛЬНИЙ ПЛАН-ПРОГРАМА

курсу підвищення кваліфікації з питань підготовки особового складу штатних підрозділів – служб захисту інформації в автоматизованих системах
(ПСЗІАС–ТР)

Київ
2024

АРКУШ ПОГОДЖЕННЯ
НАВЧАЛЬНОГО ПЛАНУ-ПРОГРАМИ
курсів підвищення кваліфікації з питань підготовки особового складу штатних підрозділів – служб захисту інформації в автоматизованих системах
(ПСЗІАС–ТР)

ПОГОДЖЕНО
Директор Департаменту військової освіти і науки Міністерства оборони України

Володимир МІРНЕНКО
"30" 09 2024 року

ПОГОДЖЕНО
Начальник Центрального управління військової освіти і науки Генерального штабу Збройних Сил України
полковник

Олег ПАВЛОВСЬКИЙ
"27" 09 2024 року

Розроблено і внесено

Голова робочої групи
Начальник служби захисту інформації в автоматизованих системах Головного Управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України
полковник Георгій КОНДРАТЬЄВ

"20" вересня 2024 року

ПЕРЕДМОВА

РОЗРОБЛЕНО робочою групою:

Головного управління зв’язку та кібербезпеки Генерального штабу Збройних Сил України.

Наказ начальника Головного управління зв’язку та кібербезпеки Генерального штабу Збройних Сил України – начальника зв’язку та кібербезпеки Збройних Сил України від 23 серпня 2024 року № 187/нагд.

Голова робочої групи:

КОНДРАТЬЄВ Георгій Анатолійович – начальник служби захисту інформації в автоматизованих системах Головного Управління зв’язку та кібербезпеки Генерального штабу Збройних Сил України, полковник.

Члени робочої групи:

КЛІМОВИЧ Сергій Олегович – начальник кафедри захисту інформації в телекомунікаційних системах та мережах Військового інституту телекомунікацій та інформатизації імені Героїв Крут, кандидат технічних наук, полковник.

БАЛАН Андрій Васильович – викладач кафедри захисту інформації в телекомунікаційних системах та мережах Військового інституту телекомунікацій та інформатизації імені Героїв Крут, майор.

Враховано:

1. Досвід підготовки та застосування військ (сил), перспектив розвитку Збройних Сил України, процедур і стандартів, прийнятих у збройних силах держав-членів НАТО.
2. Досвід ведення бойових дій.
3. Окремі доручення начальника Генерального штабу Збройних Сил України за результатами роботи груп контролю за захистом інформації та кібербезпеки пунктів управління Генерального штабу Збройних Сил України.

ЗМІСТ

1. Організаційно-методичні вказівки…….....6
2. Розподіл годин за темами (навчальними дисциплінами)……..8
3. Програма курсу (тем, навчальних дисциплін)……...…… 9

1. ОРГАНІЗАЦІЙНО-МЕТОДИЧНІ ВКАЗІВКИ

Навчальний план-програма курсу підвищення кваліфікації з питань підготовки особового складу штатних підрозділів – служб захисту інформації в автоматизованих системах військових організаційних структур Збройних Сил України є набуття знань, вмінь та практичних навичок щодо планування, організації, проведення робіт зі створення (модернізації) та контроль за їх виконанням під час експлуатації, комплексних систем захисту інформації в автоматизованих системах військових організаційних структур Збройних Сил України, забезпечення захисту інформації на автоматизованих робочих місцях, персональних електронно-обчислювальних машинах, планшетних комп'ютерах, мобільних комунікаційних пристроях тощо (далі – АС).

Категорія тих, хто навчається: офіцери, призначені на штатні посади особового складу штатних підрозділів – служб захисту інформації в автоматизованих системах військових організаційних структур Збройних Сил України.

Загальний розрахунок навчального часу проведений за наступних умов:

календарний обсяг часу підготовки складає три навчальних тижня, разом – 132 академічних годин, з них: під керівництвом – 102 годин (вхідний контроль – 2, підсумковий контроль – 6), самостійна робота та тренування – 30 годин.

Вхідний контроль передбачає проведення тестування для визначення рівня знань за фахом та проводиться на першому занятті.

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

Активними формами навчання під час засвоєння навчального плану-програми є практичні заняття з відпрацювання документів та налаштування політик та параметрів безпеки в АС. Інтенсифікація навчання і розвиток творчих здібностей досягається шляхом створення на заняттях нестандартної обстановки й відтворення проблемних ситуацій, відпрацюванням ситуаційних задач.

Поточний контроль здійснюється шляхом здачі практичного завдання.

Перевірка успішності і якості підготовки слухачів здійснюється у ході підсумкового контролю. Підсумковий контроль здійснюється у вигляді заліку. На залік відводиться 6 години за рахунок загального бюджету навчального часу. Залік повинен передбачати комплексну перевірку знань та умінь слухачів за темами підготовки.

2. РОЗПОДІЛ ГОДИН ЗАТЕМАМИ (НАВЧАЛЬНИМИ ДИСЦИПЛІНАМИ)

№ з/п	Найменування тем	Загальний обсяг (годин)		
		всього	аудиторних	самостійної роботи
1	Вхідний контроль	2	2	
2	Нормативно-правові основи інформаційної безпеки. Служба захисту інформації.	14	10	4
3	Технічний захист інформації та створення комплексу технічного захисту інформації (КТЗІ).	32	24	8
4	Кібербезпека	54	42	12
5	Створення комплексної системи захисту інформації в ІКС (АС). Порядок впровадження КСЗІ в АС класу “1” побудованих на базі організаційно-технічного рішення.	24	18	6
6	Підсумковий контроль	6	6	
Всього годин		**132**	**102**	**30**

3. ПРОГРАМАКУРСУ (ТЕМ, НАВЧАЛЬНИХ ДИСЦИПЛІН)

Загальна мета курсу підвищення кваліфікації:

Метою курсу підвищення кваліфікації набуття знань, вмінь та практичних навичок щодо планування, організації, спрямування, проведення робіт та контролю за їх виконанням під час створення (модернізації) комплексних систем захисту інформації в АС військових організаційних структур ЗС України;

проєктування, впровадження та супровід комплексних систем захисту інформації військових організаційних структур ЗС України;

забезпечення захисту інформації в АС військових організаційних структур ЗС України, а також забезпечення захисту інформації в зоні бойових дій.

В результаті підготовки на курсі підвищення кваліфікації слухач отримує:

знання:

систему нормативно-правових актів та відомчих документи що регламентують питання захисту інформації;

вимоги щодо відпрацювання необхідної документації для введення в експлуатацію та забезпечення роботи АС, організації підготовки та підвищення кваліфікації користувачів АС з питань захисту інформації, виконання заходів з реагування на кіберзагрози та кіберінциденти;

правила поводження із зовнішніми носіями інформації та використання АВПЗ;

порядок виконання робіт зі створення комплексного ТЗІ, КСЗІ в АС та керування ними, документи, якими визначений порядок налаштування політик та параметрів безпеки АС, пристроїв електронних комунікацій тощо;

уміння:

організовувати та контролювати відпрацювання необхідної документації для введення в експлуатацію та забезпечення роботи АС, створення КСЗІ АС та керування ними;

налаштовувати політики та параметри безпеки АС, пристроїв електронних комунікацій тощо;

забезпечувати контроль за дотриманням вимог нормативних документів в сфері захисту інформації щодо АС та визначених політик безпеки;

виконувати заходи з реагування на кіберзагрози та кіберінциденти, відпрацьовувати рекомендації щодо їх запобігання.

Організаційно-методичні вказівки:

Обов’язковим є систематичне закріплення набутих в ході вивчення навчального плану-програми знань та умінь під час практичних, групових занять і самостійної підготовки.

Навчальний матеріал, передбачений для вивчення під час самостійної підготовки опрацьовується відповідно до визначеного часу і виноситься на поточний та підсумковий контроль разом з навчальним матеріалом, який опрацьовується на навчальних заняттях під керівництвом науково-педагогічного працівника.

Під час проведення всіх форм занять використовуються активні методи навчання, індивідуальні, групові та фронтальні методи контролю знань. Поточний контроль проводиться у формі усного опитування або письмового експрес-контролю під час проведення навчальних занять, включаючи електронні опитувальники в різних формах за рішенням науково-педагогічного працівника – керівника занять.

Для проведення всіх видів занять використовуються такі засоби: навчальні приміщення, комп'ютерні класи, мультимедійне обладнання, наочні засоби навчання, письмове приладдя, платформи дистанційного навчання, електронні посібники, опитувальники за рішенням науково-педагогічного працівника – керівника занять.

Матеріально-технічне забезпечення:

1. Об'єкт інформаційної діяльності;
2. Навчально-тренувальний комплекс кібербезпеки;

Інформаційно-методичне забезпечення:

1. Балан А.В., Клімович С.О., Толстих В.А., Загоровець О.В., Хорошко В.О. Комплексні системи захисту інформації: проєктування, впровадження, супровід: Навчальний посібник Ч.1- К., ВІТІ, 2023. 186 с.

2. Толстих В.А., Клімович С.О., Балан А.В., Загоровець О.В., Мартинюк В.В. Системи технічного захисту інформації Навчальний посібник Ч.1- К., ВІТІ, 2023. 216 с.

3. Стандартизація та правове забезпечення інформаційної безпеки: Методичні вказівки до виконання лабораторних робіт. 2-е доп. та перероб. / М.М. Браіловський, С.О. Клімович, Б.В. Моркляник, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ФОП Ямчинський О.В., 2024. – 65с.

4. Закон України Про захист інформації в інформаційно-комунікаційних системах.

5. Закон України Про основні засади забезпечення кібербезпеки України.

6. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 (зі змінами).

7. Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93 (зі змінами).

8. Положення затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.01.2023 № 01т, зареєстроване в Міністерстві юстиції України 23 січня 2023 року за № 147/39203.

9. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 07.04.2016 № 41/ДСК.

10. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22.

11. НД ТЗІ 2.5-008-02 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.12.2002 № 84.

12. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22.

13. НД ТЗІ2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22.

14. НД ТЗІ2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджена наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22.

15. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04.12.2000 № 53.

16. НД ТЗІ 3.7-003-23 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 09.03.2023 № 924.

17. Інструкція з організації технічного захисту інформації у Збройних Силах України, затверджена наказом Головнокомандувача Збройних Сил України від 07.05.2024 № 187/ДСК.

18. Порядок впровадження КСЗІ в АС класу “1” побудованих на базі організаційно-технічного рішення, затверджений начальником Центрального управління охорони державної таємниці та захисту інформації Генерального штабу від 20.06.2024.

19. Методичні рекомендації щодо конфігурування параметрів безпеки операційної системи Windows 10 Professional в типовій автоматизованій системі класу “1”, затверджені начальником Центрального управління охорони державної таємниці та захисту інформації Генерального штабу Збройних Сил України 11 лютого 2017 року.

20. Наказ Міністерства оборони України “Про затвердження Інструкції з організації антивірусного захисту в інформаційно-телекомунікаційних системах Міністерства оборони України та у Збройних Силах України” від 26 липня 2017 року № 391.

21. Наказ командира військової частини А0106 від 10.02.2021 № 83/нагп “Про затвердження Класифікації інцидентів кібербезпеки та порушень захисту інформації в інформаційно-телекомунікаційних системах, системах спеціального зв’язку ЗС України”.

22. Наказ Міністерства оборони України від 28.12.2016 № 727 “Про затвердження Порядку використання мережі Інтернет у системі Міністерства оборони України” (зі змінами, внесеними наказом Міністерства оборони України від 03.03.2018 № 99).

23. Наказ Головнокомандувача Збройних Сил України від 23 жовтня 2021 року № 322 “Про затвердження Інструкції з організації реагування на інциденти кібербезпеки у Збройних Силах України”.

24. НД ТЗІ 1.6-005-13. Положення про категоріювання об’єктів, де циркулює інформація з обмеженням доступу, що не становить державної таємниці, затверджений наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 15.04.2013 № 215.

25. Тимчасові методичні рекомендації щодо конфігурування параметрів безпеки операційних системи Windows від 26.09.2023 № 382/42/5305;

26. Інструкція з використання зовнішніх носіїв інформації у Збройних Силах України, затверджена наказом Головнокомандувача Збройних Сил України від 05.07.2023 №189;

27. Порядок використання комп’ютерних програм у Збройних Силах України, затверджений Головнокомандувачем Збройних Сил України від 27.07.2022 № 27727/С.

28. Інструкція з налаштування засобів ідентифікації та блокування зовнішніх носіїв інформації у Збройних Силах України.

29. Наказ ГК ЗС України від 15.01.2021 N11 Про затвердження порядку отримання електронних довірчих послуг у Збройних Силах України.

30. Комплексна система захисту інформації. Інструкція з адміністрування АРМ користувача захищеної СЕДО.

31. Комплексна система захисту інформації. Інструкція користувача захищеної СЕДО.

32. Комплексна система захисту інформації. Положення відповідального за захист інформації захищеної СЕДО.

33. Комплексна система захисту інформації. Інструкція щодо порядку розгортання, підключення до сервісного сегменту СЕДО та забезпечення функціонування АРМ користувача захищеної СЕДО.

34. Комплексна система захисту інформації. План захисту інформації на АРМ користувачів захищеної СЕДО.