МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
ІМЕНІ ГЕРОЇВ КРУТ

НАВЧАЛЬНА ПЛАН-ПРОГРАМА

професійного курсу підготовки персоналу підрозділів кіберзахисту

Київ – 2021

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЗАТВЕРДЖУЮ
Командувач Військ зв'язку та кібербезпеки
Збройних Сил України
генерал-майор
Євген СТЕПАНЕНКО
"03" 01 2021 року

НАВЧАЛЬНА ПЛАН-ПРОГРАМА

професійного курсу підготовки персоналу підрозділів кіберзахисту

Категорія тих, хто навчається: військовослужбовці підрозділів відповідальних за кібербезпеку, призначені (зараховані до резерву кандидатів для просування по службі) на відповідні посади

АРКУШ ПОГОДЖЕННЯ
навчальної план-програми професійного курсу підготовки персоналу підрозділів кіберзахисту

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 персоналу підрозділів кіберзахисту Збройних Сил України, призначені для військовослужбовців підрозділів відповідальних за кібербезпеку, призначені (зараховані до кадрового резерву для просування по службі) на відповідні посади здійснюється з метою забезпечення та організації кіберзахисту в ЗС України.

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 шести змістовних модулів.

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

Всього на навчання відведено 240 годин протягом 12-ти тижнів, з них:

а) під керівництвом викладача виділяється 144 години, з них 96 годин теоретична частина, практична частина 48 годин.

б) на самостійну підготовку слухачів виділяється усього 96 годин.

в) перевірка успішності та особистої підготовки слухачів проводиться під час складання слухачами екзамену в кінці терміну навчання – 6 години.

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

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

знати, як забезпечувати мережну безпеку сучасних інформаційно-телекомунікаційних мереж та систем;

знати, як будувати та забезпечувати захист систем та мереж в глибину, розуміти порядок реалізації та здійснення атак;

знати основні принципи управління загрозами безпеки інформації в ІТС ЗСУ;

знати, як правильно застосовувати системи та алгоритми криптографічного захисту інформації, керування ризиками та реагування кіберінциденти;

знати та розуміти, як правильно налаштовувати системи безпеки Windows, Linux.

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

здійснювати налаштування та конфігурування SIEM Splank;

здійснювати налаштування та створення правила сканування мережним сканерами;

здійснювати налаштування та конфігурування програмні та програмно-апаратні пристрої міжмережної фільтрації трафіку;

здійснювати налаштування та конфігурування програмно-апаратних засобів створення VPN-тунелів;

здійснювати налаштування та конфігурування політик безпеки серверів та маршрутизаторів в ІТС ЗСУ;

здійснювати налаштування політик безпеки та правил фільтрації Windows, Linux;

здійснювати налаштування та проведення тестування уразливостей комп'ютерних мереж програмними та програмно-апаратними засобами.

Курс складається з групових та практичних занять за тематикою відповідно до наступних змістових модулів:

Змістовий модуль 1. Основи мережної безпеки.

Змістовий модуль 2. Оцінювання наявності вразливостей, загроз, ризиків та дій порушника в кіберпросторі.

Змістовий модуль 3. Управління загрозами.

Змістовий модуль 4. Криптографія, управління ризиками та реагування.

Змістовий модуль 5. Здійснення моніторингу та аналізу поведінки кінцевих користувачів.

Змістовий модуль 6. Безпека Linux.

Активними формами навчання під час засвоєння навчальної програми є практичні заняття з використанням програмних засобів, призначених для:

тестування мереж на уразливості,

аналізу трафіку,

детектування кіберзагроз,

криптографічного захисту інформації,

побудови та налаштування vpn-тунелів,

розробки програмних засобів з використанням середовища Visual Studio,

платформи віртуалізації та іншого необхідного СПЗ безкоштовного для використання в некомерційних цілях.

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

Підсумковий контроль здійснюється на заліку, який проводиться наприкінці періоду навчання.

ІІІ. ЗВЕДЕНІ ДАНІ З БЮДЖЕТУ ЧАСУ НА НАВЧАЛЬНИЙ КУРС

3.1. Розподіл навчального часу з курсу за видами навчальних занять

Семестри	Всього годин/кредитів	З них		В тому числі за видами навчальних занять							Курсові роботи (проекти)	Індивідуальні завдання	Вид та. форми контролю
		Аудиторних годин	Самостійна робота	Лекції	Семінарські заняття	Групові заняття	Групові вправи	Лабораторні заняття	Практичні заняття	Тактичні (тактико-спеціальні) заняття			
	240/8	144	96			96			48				
Разом	**240/8**	**144**	**96**			**96**			48				екзамен

3.2. Змістовий план вивчення курсу

№ з/п	Види НЗ	Кількість годин	Із них		Номери семестрів, назва змістового модуля, тем занять, навчальні питання	Відповідальний за проведення	Місце проведення
			Аудиторних годин	Самостійна робота			
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”							

IV. ФОРМИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Робочою програмою курсу підвищення кваліфікації не передбачено індивідуальних завдань.

V. ІНФОРМАЦІЙНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. Мазулевський О.Є. Захист інформації в телекомунікаційніх системах і мережах: навч.посібник . Ч.І / О.Є. Мазулевський , І.В. Самойлов, А.С. Шевченко. – К.: ВІТІ, 2015, - 260 с.

2. Грайворонський М.В., Новіков О.М. Безпека інформаційно- комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.

3. Поповский В.В. Защита информации в телекоммуникационных системах: учебник: в 2-х т. / В.В. Поповский, А.В. Персиков, - Х.: ООО «Компания СМИТ», 2006, Т.1. – 238 – с. Т.2 – 292 с.

4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2012. – 544 с.

5. Ленков С.В. Методы и средства защиты информации в 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А., Под редакц. В.А. Хорошко. – К.: Аррий, 2008, - том. – 1. Несанкционированное получение информации. – 464 с.

6. Богомолова О.Б. Защита компьютера от вредоносных воздействий: практикум / О.Б. Богомолова, Д.Ю. Усенков. – М.: БИНОМ. Лаборатория знаний, 2012. – 175 с.

7. Ачилов Р.Н. Построение защищенных корпоративных сетей / Р.Н. Ачилов. – М.: ДМК Пресс, 2013. – 250 с.

8. Соколов А.В. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М,: ДМК Пресс, 2002. – 656 с.:

9. Лебедев А. Защита компьютера от вирусов, хакеров и сбоев: понятный самоучитель / А. Лебедев, С-Пб: Питер, 2013, - 158 с.

10. Куприянов А.И. и др. Основы защиты информации: Учебное пособие / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – М.: Издательский центр Академия, 2008, - 256 с.

11. Корш А.П. Антивирусы: компьютерная шпаргалка / А.П. Корш, П.П. Алексеев, Р.Г. Прокди. – СПб.: Наука и техника, 2010, - 80 с.

12. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: коллективн. моногр. / под ред. В.М. Безрука, В.В. Баранника, - Х.: Компания СМИТ, 2013, - 398 с.:

13. Разумовский Н.Т. Бесплатные антивирусы для вашего компьютера + Бесплатное использование платных антивирусов / Н.Т .Разумовский, А.П. Борц, Р.Г. Прокди. – 3-е изд. – СПб: Наука и техника, 2010. – 192 с.:

14. Чипига А.Ф. Информационная безопасность автоматизированных систем. Учеб.пособие для студентов вузов и обучающихся по специальностям в обл.информ.безопасности / А.Ф. Чипига, - М. Гелиос АРВ, 2010, - 336 с. Ил.

15. Моримото Р. Windows Server 2008 R2. Полное руководство. / Р. Моримото, М. Ноэл, О. Драуби, Р. Мистри, К. Амарис. – М.: Виьямс, 2012.– 1456 с.

16. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. Учеб.пособ. для студентов высш.учеб. заведений / П.Б. Хорев. – 4-е изд. Стер. – М. Издательский центр «Академия», 2008. – 256 с.

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