Ընդհանուր դասընթացների քանակ	Շաբաթական դասընթացների քանակ	Մեկ դասընթացի տևողություն	Ընհանուր դասընթացների ժամաքանակ	Տեսական դասընթացների ժամաքանակ	Գործնական դասընթացների ժամաքանակ
27	3	2	54	29	25

«Կիբեռանվտանգություն» դասընթացի ծրագիր

Հ/Հ	Դաս	Դասավանդող դասախոս	Դասընթացի նկարագրություն		Ժամերի քանակ	
			Գործնական	Տեսական	Գործ.	Տես.
Ընդ.	**Միջին մակարդակի դասընթաց**					
	Կիբերանվտանգություն. Փորձագետների և կրիմինա աշխարհ:	Ա. Չիբուխչյան Հ. Խաչատրյան	• Կիբերանվտանգության ոլորտի աշխատանքի փնտրում: • Սպառնալիքների նույնականացում: • Կիբերանվտանգության մասնագետների աշխարհ: • Կիբերաշխարհի ստեղծում: Հաղորդակցում կիբերմիջավայրում:	- Կիբերանվտանգության աշխարհը, - Կիբերանվտանգության դոմենները, - Կիբերկրիմինալն ընդդեմ կիբերանվտանգության մասնագետների, - Կիբերանվտանգության կրիմինալը, - Կիբերանվտանգության մասնագետները, - Ընդհանուր սպառնալիքներ, - Սպառնալիքների ասպարեզները, - Կիբերանվտանգության սպառնալիքների տարածումը, - Ի՞նչպես են տարածվում սպառնալիքները,	4	4

				- Սպառնալիքները բարդությունը, - Փորձագետների պատրաստում, - Կիբերանվտանգության աշխատանքային շուկան, - Կիբերանվտանգության առցանց համայնքները, - Կիբերանվտանգության որորտի սերտիֆիկացումները:		
	Կիբերանվտանգության խորանարդը:	Ա. Չիբուխչյան Հ. Խաչատրյան	• Վիրտուալ մեքենայի տեղադրում անհատական համակարգչում: • Վավերացում, թույլտվություն և հաշվառում: • Ֆայլերի և տվյալների գաղտնագրում: Ֆայլերի և տվյալների ամբողջականության ստուգում:	- Կիբերանվտանգության խորանարդի երեք չափումները, - CIA եռյակ, - Գաղտնիություն, - Ամբողջականություն, - Հասանելիություն, - Տվյալների կարգավիճակներ, - Data at Rest, - Data In-Transit - Data in Process, - Կիբերանվտանգության հակամիջոցները, - Տեխնոլոգիաներ, - Կրթություն, իրազեկում և ուսուցում, - Կիբերանվտանգության քաղաքականությունները և ընթացակարգերը,	4	3

				- SS անվտանգության կառավարման կառուցվածքը, - ISO կիբերանվտանգության մոդելը և նրա կիրառումը:		
	Կիբերանվտանգության սպառնալիքներ, խոցելիություններ և հարձակումներ:	Ա. Չիբուխչյան Հ. Խաչատրյան	• Սպառնալիքների և խոցելիությունների հայտնաբերում: • WEP/WPA2 PSK/WPA2 RADIUS կոնֆիգուրացում:	- Վնասակիր ծրագրեր և կոդեր, - Վնասակիր ծրագրերի տեսակներ, - էլ. Փոստի և վեբ-դիտարկիչների հարձակումներ, - Խոցելիություններ, - Խաբեություն, - Խաբեության արվեստը, - Խաբեության մեթոդները, - Հարձակումներ, - Կիբերհարձակումների տեսակներ, - Անլար և շարժական սարքերի նկատմամբ հարձակումները, - Կիրառական ծրագրերի հարձակումներ:	4	4
	Գաղտնիքների պաշտպանման արվեստը:	Ա. Չիբուխչյան Հ. Խաչատրյան	• Ստեգանոգրաֆիայի օգտագործում: • Տրանսպորտային ռեժիմի VPN-ի կարգաբերում:	- Կրիպտոգրաֆիա (ծածկագիտություն), - Անձնական բանալիով ծածկագրում, - Հանրային բանալիով ծածկագրում, - Սիմետրիկ և ասիմետրիկ ծածկագրում,	4	4

			Թունելային ռեժիմի VPN-ի կարգաբերում:	- Հասանելիության հսկում, - Հասանելիության հսկման տեսակներ, - Հասանելիության հսկման ստրատեգիաներ, - Նույնականացում, - Վավերացման մեթոդներ, - Թույլտվություն, - Accountability, - Անվտանգության հսկման տեսակներ, - Տվյալների քողարկում, - Տվյալների դիմակավորում, - Ստեգանոգրաֆիա:		
	Ամբողջականության ապահովման արվեստը:	Ա. Չիբուխչյան Հ. Խաչատրյան	• Գաղտնաբառերի կոտրում: • Թվային ստորագրությունների օգտագործում: • Հեռահար հասանելիություն	- Տվյալների ամբողջականության հսկման միջոցների տեսակները, - Հեշավորման ալգորիթմներ, - Salting, - HMAC, - Թվային ստորագրություններ, - Ստորագրություններ և օրենքները, - Ի՞նչպես են թվային ստորագրությունները աշխատում, - Սերտիֆիկատներ,	4	4

				- Թվային սերտիֆիկատների հիմունքներ, - Թվային սերտիֆիկատի կառուցում, - Տվյալների շտեմարանների ամբողջականության ապահովումը, - Տվյալների շտեմարանների ամբողջականություն, - Տվյալների շտեմարանների վավերացում, - Տվյալների շտեմարանների ամբողջականության պահանջները:		
	Հինգ իննների հասկացողությունը:	Ա. Չիբուխչյան Հ. Խաչատրյան		- Բարձր հասանելիություն, - Հինգ իններ, - Հասանելիության բարելավման միջոցները, - Ակտիվների կառավարում, - Խորը պաշտպանություն, - Ավելորդություն, - Համակարգերի առաձգականություն, - Միջադեպերի արձագանքում, - Արձագանքման փուլեր, - Արձագանքման տեխնոլոգիաներ, - Վերականգնում աղետներից,		3

				- Աղետներից վերականգման պլանավորում, - Բիզնեսի շարունակականության պլանավորում:		
	Կիբերանվտանգության դոմենի պաշտպանում:	Ա. Չիբուխչյան Հ. Խաչատրյան	• Linux օպերացիոն համակարգի ամրացում: Սերվերների ֆայրվոլներ և երթուղիչների ACL-ներ:	- Համակարգերի և սարքերի պաշտպանում, - Հոստերի ամրացում, - Անլար և շարժական սարքերի ամրացում, - Հոստերի տվյալների պաշտպանում, - Պատկերներ և բովանդակության հսկում, - Աշխատանքային կայանների ֆիզիկական պաշտպանում, - Սերվերների ամրացում, - Անվտանգ հեռահար հասանելիություն, - Ադմինիստրատիվ միջոցներ, - Սերվերների ֆիզիկական պաշտպանում, - Ցանցի ամրացում, - Ցանցային սարքերի անվտանգություն, - Ձայնային և վիդեո սարքավորումներ, - Ֆիզիկական անվտանգություն, - Ֆիզիկական հասանելիության հսկում,	4	4

				- Հսկողություն:		
	Մուտք կիբերանվտանգու- թյան մասնագետների համայնք:	Ա. Չիբուխչյան Հ. Խաչատրյան	Գիտելիքների ինտեգրման մարտահրավեր:	- Կիբերանվտանգության դոմեններ, - Օգտատիրոջ դոմեն, - Սարքի դոմեն, - Տեղային ցանցի դոմեն, - Անձնական ամպի դոմեն, - Հանրային ամպի դոմեն, - Ֆիզիկական տարածքների դոմեն, - Ծրագրերի դոմեն, - Կիբերանվտանգության ոլորտի էթիկայի և պատասխանատվության հասկացողություն, - Էթիկայի սկզբունքներ, - Կիբերօրենքներ և պատասխանատվություն, - Կիբերանվտանգության տեղեկատվության կայքեր, - Կիբերանվտանգության զենքեր, - Հետագա քայլերը, - Կիբերանվտանգության մասնագիտության ուսումնասիրում:	1	3

Դասընթացի ավարտին ի՞նչ գիտելիքների է տիրապետելու մասնակիցը:

- Հասկանալ ցանցերի, սերվերների և հավելվածների անվտանգության վերահսկումը:
- Սովորել անվտանգության արժեքավոր սկզբունքները և ինչպես մշակել համապատասխան քաղաքականություն:
- Իրականացնել տվյալների գաղտնիության և մատչելիության պատշաճ ընթացակարգեր:

- Զարգացնել քննադատական մտածողություն և խնդիրներ լուծելու հմտություններ՝ օգտագործելով իրական սարքավորումներ և Cisco Packet Tracer:
- Հասկանալ հաքերների մտածողությունը: Սովորել դիմակայել կիբեռհարձակումներին:
- Ուսումնասիրել կիբեռանվտանգության մասնագետների աշխատանքային շուկան:
- Հասկանալ կիբեռ և տեղեկատվական անվտանգության ստանդարտները:
- Սովորել տվյալների ամբողջականության, գաղտնիության և հասանելիության ապահովման գործիքներն ու ընթացակարգերը:
- Ոսումնասիրել կիբեռ հարձակումների տեսակներն ու դրանց դեմ պայքարի միջոցները:

Դասընթացի արդյունքում ձեռք են բերվում վերամասնագիտական փափուկ հմտություններ (**soft skills**):
Դասընթացի ընթացքում մասնակիցները ծանոթանում են ոլորտի իրավական և էթիկական կանոններին, ձեռք են բերում համատեղ աշխատանքի, խնդիրների լուծման ինչպես նաև վերլուծական մտածողության հմտություններ: