УЧЕБНА ПРОГРАМА

Код:	**91-308-23**	Дисциплина:	**Киберсигурност**
Ниво:	6Б. Бакалавър	ECTS кредити:	**6**
Обучаващо звено:	катедра Обществен ред и сигурност		

Анотация на учебната дисциплина

Учебната дисциплина „Киберсигурност” е задължителна за специалности "Защита на националната сигурност" и “Противодействие на престъпността и опазване на обществения ред" в ПН 9.1 Национална сигурност на ВСУ “Черноризец Храбър”. Тя обхваща основни теоретични възгледи за същността, съдържанието, особеностите и правната регламентация на информационната и киберсигурност. Включва пет концентрично разположени и взаимно обусловени групи от проблеми. На *първо място* са тези, свързани със същността и спецификите на проблемите в глобалното информационно пространство, историческите аспекти на развитието на науката за информационна и киберсигурност, сложният спектър от понятия в терминологичния апарат на дисциплината и техните характеристики. *Вторият кръг* проблеми третира въпросите за мястото и ролята на киберсигурността в системата за защита на националната сигурност. Разгледани са правните и организационните аспекти на киберсигурността в Р България, особеностите при защитата на критичната информационна инфраструктура, военни и гражданскоправни аспекти на киберсигурността. Поставен е акцент върху международното сътрудничество в киберсигурността, кибердипломацията и политика на ЕС за защита при киберкризи. *Трета група* са въпросите, подчинени на технологичните аспекти на уязвимостите и заплахите в киберпространството, класификациите на заплахите и уязвимостите и управлението на риска. *Четвъртата група* въпроси са посветени на посегателствата срещу киберсигурността и компютърната престъпност (киберпрестъпност). Разгледани са основните мотиви за посегателство върху информационната и киберсигурност, генезисът на феномена “компютърна престъпност” и негови характерни черти, класификацията на компютърните престъпления, обща характеристика и наказателноправни аспекти. Поставен е акцент върху водещата роля на координацията и взаимодействието между отделните държави, международните организации и специализираните националните органи за противодействие на киберпрестъпността. Заключителната *пета група* въпроси цели да запознае обучаемите със стандартизацията в областта на информационната и киберсигурност и нейното приложение в практиката като полезен инструмент за осигуряване на информационната и киберсигурност в организацията.

Компетентности като очаквани резултати от обучението

Знания:	за същността и спецификите на проблемите в глобалното информационно пространство; за развитието на науката за информационна и киберсигурност; за мястото и ролята на киберсигурността в системата за защита на националната сигурност; за правните и организационните аспекти на киберсигурността в Р България; за особеностите при защитата на критичната информационна инфраструктура; за технологичните аспекти на уязвимостите и заплахите в киберпространството, класификациите на заплахите и уязвимостите и управлението на риска; за посегателствата срещу киберсигурността и компютърната престъпност (киберпрестъпност); за класификацията и характеристиките на компютърните престъпления; за подходите в противодействието на киберпрестъпността; за използваните стандарти в областта на информационната и киберсигурност.
Умения:	за оценка, анализ и управление на информационната и киберсигурност и защитата на информацията в организацията; за бързо и адекватно реагиране на промените, конфликтите и кризите в киберпространството; за разграничаване, идентифициране и подбор на подходящи организационни и управленски мерки за трансформиране на организациите, в съответствие с възникналите ситуации, заплахи и рискове за киберсигурността; за използване и прилагане в различни държавни и частни структури на международни стандарти за информационна и киберсигурност.

Отношения и нагласи: за концептуално мислене в сферата на защита на киберсигурността и защитата на информационната и мрежова сигурност; за вземане на стратегически решения в тази област; за успешно реагиране при нови ситуации и нетрадиционни заплахи; за анализ и разработка на оперативна концепция, системен модел и изисквания за внедряване на система за информационната и киберсигурност в държавни и частни структури.

Методи за обучение и връзки с други дисциплини

Методи на обучение: Лекции, семинарни упражнения, дискусии, консултации (вкл. онлайн), самостоятелна работа с нормативни източници, изследователска работа за изготвяне на курсов проект.

Предварителни изисквания: Усвояването на знанията по дисциплината "Киберсигурност" предполага наличието на познания по „Информатика" и „Информационни системи и технологии", а също така и по някои базови за специалността учебни дисциплини като "Правото на сигурност",„Анализ и контрол на риска", „Теория на управлението" и др.

Осигурявани дисциплини: Задължителни и задължително избираеми дисциплини за специалността.

Проверка на знанията и уменията

Крайно оценяване: Семестриален изпит по шестобалната система и ECTS. Окончателната оценка се формира от самостоятелно подготвен курсов проект, текущи оценки от контролна работа и задачи, поставени по време на семинарните упражнения, както и от резултатите от писмен изпит (тест) в края на обучението.

Методи и форми на оценяване: Писмен изпит (тест), контролна работа и кратки задачи (текущи оценки), защита на курсов проект чрез презентационен материал, курсов проект, участие в дискусии.

Критерии за оценяване: До изпит се допуска студент, който е участвал пълноценно в учебния процес, преминал е текущ контрол с положителна оценка и е подготвил курсов проект. При постигане на значими резултати от конкретното изследване за целите на курсовия проект, от които е видно, че студентът е усвоил съдържанието на лекционния курс и е показал умение да го прилага, може да бъде освободен от явяването на изпит с много добра или отлична оценка. Необходимо е оценката от контролната работа да бъде много добра или отлична.

"ОТЛИЧЕН": Студентът показва всестранни и задълбочени знания, дава обосновани и точни отговори по въпросите, умело, логично и точно излага мислите си, притежава практически умения и навици по отчитане на кризисните ситуации. Висока степен на критично мислене. Притежава познания и способности при прилагане на наученото. Балансирано представя най-важните тезисни позиции. Успешно излага убедителни доказателства, както в полза, така и срещу изразеното мнение в случаите на анализ. Доказателственият материал е подкрепен ясно, точно и убедително с цитиране на нормативни актове. Заключителната част изразява ясно становище на студента по въпроса, при това с прецизна терминология и литературна езикова компетентност.

"МНОГО ДОБЪР": Студентът има пълни и задълбочени познания, притежава практически умения, има логична и задълбочена мисъл, умело си служи с правната терминология. По голямата част от информацията е умело разгърната. Доказателственият материал е подкрепен ясно, точно и убедително с цитиране на нормативни актове. Съществува леко нарушаване на баланса при представяне на основните аргументи. Заключителната част изразява ясно становище на студента по въпроса, при това с прецизна терминология. Допускат се отделни езикови неточности.

	"ДОБЪР": Студентът има пълни знания, притежава практически умения, има задълбочена мисъл, умело си служи с правната терминология. Преобладава описанието вместо аналитичното мислене. Отговорът съдържа основна информация, но с леко нарушен баланс при представянето й. Доказателственият материал е подкрепен ясно, точно и убедително с цитиране. От заключителната част се разбира становището на студента. Допускат се отделни езикови неточности. "СРЕДЕН": Студентът отговаря по същността на въпросите с известни затруднения, има недостатъчни практически умения и навици, не винаги излага точно мислите си. Доказателственият материал е представен по разбираем, но неправилно структуриран начин. Някои от аргументите са неправилно разбрани, но като цяло същността е ясна. Съществува опит за оформяне на заключение, но позицията на студента остава неясна. Съществуват пропуски и езикови неточности. "СЛАБ": Студентът няма необходимите знания, допуска принципни грешки, затруднява се в отговорите, не умее да обясни същността на въпроса. Недостатъчен обем от информация. В представянето на информацията липсва добра аргументация. Цитирането е неправилно. Наблюдават се груби грешки.
Компоненти и тяхната тежест в крайната оценка:	Първи вариант - при явяване на изпит: активно участие в лекции, семинарни упражнения и дискусии - 10%; самостоятелно подготвена и защитена курсова работа - 40%; текуща оценка от контролна работа и/или кратки задачи - 20%; резултати от писмен изпит в края на обучението - 30%. Втори вариант - при освобождаване от явяване на финален семестриален изпит: участие в лекции, семинарни упражнения и дискусии - 20%; самостоятелно подготвена и защитена курсова работа - 60%; текуща оценка от контролна работа - 20%.

Учебни материали и ресурси за самоподготовка

Основна литература:

1. Актуализирана стратегия за национална сигурност на Р България, приета с Решение на НС от 14.03.2018 г., обн., ДВ, бр. 26 от 23.03.2018 г.
2. Актуализирана Национална стратегия за киберсигурност „Киберустойчива България 2023", приета с Решение № 301 на МС на РБ от 02.04.2021 г.
3. Актуализирана Стратегия за развитие на електронното управление в Република България 2019 – 2025 г., приета с Решение № 298 на МС на РБ от 02.04.2021 г.
4. Закон за управление и функциониране на системата за защита на националната сигурност, обн. ДВ бр. 61 от 11.08.2015 г.
5. Закон за киберсигурност, Обн. ДВ. бр.94 от 13 Ноември 2018 г.
6. Директива относно мерки за високо общо ниво на киберсигурност в Съюза (Директива за МИС2), DIRECTIVE (EU) 2022/2555
7. Наредба за минималните изисквания за мрежова и информационна сигурност, в сила от 26.07.2019 г., приета с ПМС № 186 от 19.07.2019 г., обн. ДВ. бр.59 от 26 Юли 2019 г.
8. Кръстев, Др., Правни основи на киберсигурността, I и II том, ИК "Стено", Варна, 2021 г.
9. Семерджиев, Цв., Управление на информационната сигурност, С., 2007 г.
10. Бояджиева, Ю., Компютърна престъпност, С., 2004 г.

Допълнителна литература:

1. Мичев Ст., Рискове за сигурността в информационното общество, учебно пособие, https://iniod.unibit.bg/wp-content/uploads/2015/11/%D0%A0%D0%B8%D1%81%D0%BA%D0%BE%D0%B2%D0%B5-%D0%B7%D0%B0-%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82%D1%82%D0%B0-%D0%B2-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D1%82%D0%BE-%D0%BE%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%BE.pdf
2. Николов, И., Съвременни тенденции при формиране на политики за информационна сигурност, http://conf.uni-ruse.bg/bg/docs/cp15/3.2/3.2-8.pdf
3. Туджаров, Хр., Архитектура на информационната сигурност, електронно учебно пособие, 2010 г., http://tuj.asenevtsi.com/Asec10/IndexAIS.htm
4. Пърлрот, Н., Кибервойната, ИК Кръгозор, С., 2022 г.

5. Гудман, М., Киберпрестъпления, изд. Милениум, С., 2016 г.
6. Борисов, Ат., Трансгранични престъпления, изд. Нова звезда, С., 2017 г.
7. Манасиева, А., Киберпсихология. Поведенчески аспекти, изд. Изток-Запад, 2016 г.
8. Национален портал за киберсигурност, http://ncs.nlcv.bas.bg/
9. Information and Security Journal, http://itsec.procon.bg/article/
10. Profisec, Professional Security Magazine, http://profisec.bg/bg/topic/magazine

Речник (ключови думи)

информационно общество, киберпространство, информационна система и мрежа, критична информационна инфраструктура, информационна сигурност, информационна и мрежова сигурност, киберсигурност, киберотбрана, заплахи, уязвимости, управление на риска, компютърна престъпност, киберпрестъпност, противодействие на киберпрестъпността, стандарти за управление на информационната сигурност (киберсигурност), международно сътрудничество

Съдържание на учебната дисциплина по тематични единици за редовна / задочна форма на обучение

№	Тема	Основни въпроси	Лекции	Сем. упр.	Пр. зан.	Извън аудит.	Осигуряване
1	Проблеми на глобалното информационно общество	Съдържание, обект и предмет на учебната дисциплина, изисквания. Информационно общество – същност и основни характеристики. Същност на понятията за “информационно пространство”, “информационна инфраструктура”, “глобална информационна инфраструктура”, “информационна среда”, “информационни ресурси”, сигурност (несигурност). Глобална информационна несигурност	3			6	Мултимедия, лаптоп, интернет връзка
2	Развитие на идеята за информационната сигурност	Генезис и развитие на информационната сигурност. Исторически аспекти. Съдържание и обхват на информационната сигурност като наука	3			6	
3	Терминологичен апарат на дисциплината. Същност и обхват на понятията	Същност и съдържание на понятията за “киберпространство”, “информационна сигурност”, “киберсигурност”, “киберустойчивост”, “киберзащита” и др. Категории (характеристики) на информационната и киберсигурност и тяхната същност.	2			4	
4	Информационната и киберсигурност като проблем на националната сигурност	Национална сигурност и киберсигурност. Държавна политика по гарантиране на информационната и киберсигурност.	4			8	
5	Законодателна рамка на киберсигурността в Р България	Основни нормативни актове. Стратегии, доктрини, процедури. Предотвратяване и готовност за реагиране при заплахи за киберсигурността. Демократичен контрол в сферата на киберсигурността.	4			8	
6	Организация на киберсигурността в Р България. Функции и отговорности	Основни институции в сферата на киберсигурността. Ресурсно осигуряване. Взаимодействие и координация.	2			4	
7	Киберзащита на критичната информационна инфраструктура	Същност на понятието “инфраструктура”. Същност и видове. Видове зависимости на критичната инфраструктура. Специфики на критичната информационна инфраструктура. Модел за защита на критичната инфраструктура.	2			4	
8	Киберотбрана	Същност на понятието “киберотбрана”. Операции в киберпространството. Същност и съдържание на понятието “кибервойна”. Методи и етапи на кибервойната. Видове бойни кибероперации. Кибершпионаж. Кибертероризъм. Защита.	4	5		15	
9	Гражданскоправни аспекти на киберсигурността	Онлайн нарушения на авторските права в Интернет. Видове произведения в Интернет и особености на тяхната защита. Правно регулиране на категорията “биометрични лични данни”.	2			6	
10	Международноправни аспекти на сътрудничество в областта на киберсигурността	Стратегии за киберсигурност. Кибердипломация. Политика на ЕС за защита при киберкризи.	3			6	Мултимедия, лаптоп, интернет връзка
11	Технологични аспекти на заплахите и уязвимостите в киберпространството	Класификация на уязвимостите. Класификация на заплахите (социално инженерство, мрежово-базирани заплахи, заплахи към безжичните мрежи, софтуерно-базирани заплахи).	4	3		15	

12	Уязвимост на информационната и мрежова сигурност. Оценка и управление на риска	Уязвимост на информационната сигурност, реализирана в условията на мрежа. Оценка, анализ и управление на риска в компютърните системи и мрежи.	2			4	
13	Посегателства срещу киберсигурността. Компютърна престъпност (киберпрестъпност)	Основни мотиви за посегателство върху информационната и киберсигурност. Дефиниране на понятията “компютърна престъпност”, “киберпрестъпност”. Феноменология на компютърната престъпност – генезис и същност. Характерни черти на компютърната престъпност. Класификация на определенията за компютърна престъпност. Дефиниране на понятията “компютърно престъпление”, “киберпрестъпление”. Класификация на компютърните престъпления. Обща характеристика. Наказателноправни аспекти.	5	5		20	
14	Противодействие на киберпрестъпността	Национални органи за противодействие на киберпрестъпността. Международно оперативно сътрудничество в борбата с трансграничната киберпрестъпност. Киберпространството и организацията на киберпрестъпността.	2			4	
15	Стандартизация в областта на информационната и киберсигурност	Международни стандарти и спецификации в областта на информационната и киберсигурност	3	2		10	
	Общо часове		45	15		120	

Разработил програмата: доц. д-р Галина Великова Милева, galina.mileva@vfu.bg

Учебната програма е приета от Съвета на катедра Обществен ред и сигурност с протокол № 7/28.03.2024 г.

Учебната програма е утвърдена от Факултетния съвет на Юридически факултет с протокол № 9 /04.04.2024 г. и заповед № 76/05.4.2024 г. на декана на факултета.