МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
Кафедра інформаційних технологій та кібербезпеки факультету № 4

МЕТОДИЧНІ МАТЕРІАЛИ ДО ПРАКТИЧНИХ ЗАНЯТЬ

з навчальної дисципліни **" Вступ у спеціальність "**
вибіркових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти

125 "Кібербезпека" (Безпека інформаційних та комунікаційних систем)

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (протокол від 15.09.2020 № 16)

Розробник: доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ, к.т.н. доцент Тулупов В.В.

Рецензенти:
професор кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, к.т.н. доцент Носов В.В.

професор кафедри проектування та експлуатації електронних апаратів Харківського національного університету радіоелектроніки, к.т.н. доцент Хорошайло Ю.Є.

.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та найменування тем	Кількість годин відведених на вивчення навчальної дисципліни						Література, сторінки	Вид контролю
	Всього	з них:						
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота		
Тема № 1. Законодавство в сфері забезпечення інформаційної безпеки	8	2	–	2	–	4	1,4,5-7,10,11,15,16,17,18,2021,22,26	
Тема№2. Основні положення інформаційної безпеки	6	2	–	2	–	4	11,15,18, 22,23,28,31-34,37,39	
Тема № 3. Правові питання захисту інформації з використанням технічних засобів	6	2	–	2	–	4	10,12,14,19	
Тема № 4. Загрози інформаційній безпеці, безпеці інформації та інформаційних ресурсів	6	2	–	2	–	4	10,12,14	
Тема № 5. Юридична відповідальність за порушення правових норм в сфері інформаційної безпеки	8	2	–	2	–	4	1,3-5,6,9,11,32	
Тема № 6. Загальна характеристика каналів витоку інформації	8	2	–	2	–	4	29,31	
Тема № 7. Функціональні вимоги до засобів захисту	6	2	–	2	–	4	29,31	
Тема № 8. Основи управління інформаційною безпекою	6	2	–	2	–	4	29,31	
Тема № 9. Загальні методи забезпечення інформаційної безпеки	8	2	–	2	–	4	29,31	
Тема № .10 Засадничі принципи боротьби з кіберзлочинністю	8	2	-	2		4	1,4-21	
Тема № 11. Методи боротьби з кіберзлочинністю за межами України	10	4	-	2		4	1, 22-29	
Всього	**90**	**24**		**22**		**44**		**залік**

2. Методичні вказівки до практичних занять:

Тема № 1. Законодавство в сфері забезпечення інформаційної безпеки

Практичне заняття № 1. Законодавство в сфері забезпечення інформаційної безпеки

Навчальна мета заняття: розглянути стан захищеності потреб особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх загроз.

Кількість годин: 2 год.

Навчальні питання.

1. Інформаційна безпека: поняття, структура, зміст.
2. Державна політика України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави, сучасних автоматизованих і телекомунікаційних систем.
3. Класифікація та структура нормативних правових актів в сфері інформаційної безпеки України.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.

15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
23. Про ліцензування видів господарської діяльності : Закон України від 02.03.2015 № 222-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/222-19.
24. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 05.04.2007 № 877-V // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/877-16.
25. Про акредитацію органів з оцінки відповідності : Закон України від 17.05.2001 № 2407-III // База даних «Законодавство України» / Верховна Рада України. URL https://zakon.rada.gov.ua/laws/show/2407-14:
26. Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання : Закон України від 20.02.2003 № 549-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/549-15.
27. Про наукову і науково-технічну експертизу : Закон України від 10.02.1995 № 51/95-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80.
28. Про метрологію та метрологічну діяльність : Закон України від 05.06.2014 № 1314-VII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1314-18.
29. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
30. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1229/99.
31. Про затвердження Концепції технічного захисту інформації в Україні : постанова Кабінету Міністрів України від 08.10.1997 № 1126 // База даних «Законодавство України»

/ Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF.
32. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : постанова Кабінету Міністрів України від 03.09.2014 № 411 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF.
33. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.
34. Закон України «Про електронні довірчі послуги» від 05.10.2017 р. № 2155-VIII //Відомості Верховної Ради (ВВР), 2017, № 45, ст.400.
35. Про деякі питання захисту інформації, охорона якої забезпечується державою : постанова Кабінету Міністрів України від 13.03.2002 № 281 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF.
36. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF.

Інформаційні ресурси в Інтернеті

37. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
38. Перелік нормативно-методичних документів в галузі захисту інформації // Облікові документи для секретного діловодства / ТОВ «НІКС» : офіційний вебсайт. URL: https://sites.google.com/a/nics.com.ua/price/.
39. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом // Державна служба спеціального зв'язку та захисту інформації України : офіційний веб сайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=39181.
40. Відомості про засоби технічного захисту інформації, на які закінчився термін дії сертифікатів відповідності та експертних висновків // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=234241&cat_id=39181.
41. Каталог обладнання для виявлення каналів витоку інформації // Digital and Analog Systems: офіційний вебсайт. URL: https://www.das-ua.com/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/.
42. Каталог обладнання для протидії засобам знімання інформації// Digital and Analog Systems: офіційний вебсайт. URL: https://www.das-ua.com/katalog/obladnannya-protidii-zasobam-znimannya-informacii/.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet;

медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

1. Розглянемо основні поняття. Інформаційна безпека: поняття, структура, зміст

Безпека інформаційної сфери – це ужиття комплексних заходів щодо захисту свого інформаційного простору та входження України у світовий інформаційний простір.

Під *національним інформаційним простором* розуміють усю сукупність

інформаційних потоків як національного походження, так і іноземних, що доступні на території держави.

Безпека в інформаційній сфері передбачає:

– забезпечення інформаційного суверенітету України;

– удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

– вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Під *інформаційним середовищем* розуміють сферу діяльності суб'єктів, пов'язану із створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на *три основні складові*:

– створення і розповсюдження вихідної та похідної інформації;

– формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

– споживання інформації;

та *дві забезпечувальні предметні складові*:

– створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;

– створення і застосування засобів і механізмів інформаційної безпеки.

Із врахуванням складових інформаційного середовища *інформаційна безпека* – це стан захищеності потреб особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх загроз.

2. Державна політика України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави, сучасних автоматизованих і телекомунікаційних систем

Державна політика України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави, сучасних автоматизованих і телекомунікаційних систем визначається пріоритетністю національних інтересів і має на меті унеможливлення реалізації загроз для інформації.

Метою інформаційної політики держави є створення умов для побудови в державі інформаційного суспільства як органічного сегменту глобального інформаційного співтовариства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захисту національних моральних і культурних цінностей, забезпечення конституційних прав на вільний доступ до інформації.

Основними напрямами такої політики є:

– забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси;

– формування і захист державних інформаційних ресурсів;

– розвиток законодавства у сфері інформаційних процесів, інформатизації і захисту інформації.

– створення і розвиток центральних і регіональних інформаційних систем та мереж, забезпечення їхньої сумісності і взаємодії в єдиному інформаційному просторі держави;

– створення умов для якісного і ефективного інформаційного забезпечення громадян, установ державної влади, органів місцевого самоуправління, організацій і суспільних об'єднань на основі державних інформаційних ресурсів;

– забезпечення національної безпеки у сфері інформатизації, а також забезпечення прав громадян, організацій в умовах інформатизації;

– сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій, засобів їхнього забезпечення;

– формування і здійснення єдиної науково-технічної промислової політики у сфері інформатизації з урахуванням сучасного світового рівня розвитку інформаційних технологій.

3. Класифікація та структура нормативних правових актів в сфері інформаційної безпеки України

Основою правового регулювання захисту та обмеження доступу до інформації є:

– норми ч. 1 ст. 32 Конституції України, згідно з якими не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини;

– норми ч. 2 ст. 34 Конституції України, якими передбачено можливість обмеження свободи інформації на основі закону в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Інформаційні правовідносини на рівні законодавства регулюються двома групами законодавчих актів:

1) *загальноправові акти*, дія яких поширюється на всіх суб'єктів інформаційних відносин відповідно до поділу права України на правові галузі: конституційне, адміністративне, цивільне, трудове, кримінальне;

2) *спеціально-правові акти*, дія яких поширюється тільки на суб'єктів, які беруть безпосередню участь у конкретній соціальній діяльності.

Спеціально-правові розділяються на *дві категорії,* котрі мають відповідні системоутворюючі законодавчі акти (у теорії права вони формують синтетичні міжгалузеві комплексні інститути права):

– системоутворюючі загальні норми публічно-правового регулювання інформаційних відносин (інформаційне право) в Україні – Закон «Про інформацію»;

– системоутворюючі окремі інституції інформаційного права – закони України «Про наукову і науково-технічну діяльність», «Про державну таємницю», «Про державну статистику», «Про Національний архівний фонд та архівні установи», «Про друковані засоби масової інформації (пресу) в Україні», «Про інформаційні агентства» тощо.

II. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 2. Основні положення інформаційної безпеки

Практичне заняття № 2. Основні положення інформаційної безпеки

Навчальна мета заняття: розглянути поняття про предмет, об'єкт і суб'єкти інформаційної безпеки. Види інформаційної безпеки. Концепція інформаційної безпеки держави . Державна таємниця як особливий вид інформації, що захищається.

Кількість годин: 2 год.

Навчальні питання:

1. Предмет, об’єкт і суб’єкти інформаційної безпеки.
2. Види інформаційної безпеки.
3. Концепція інформаційної безпеки держави
4. Державна таємниця як особливий вид інформації, що захищається.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв’язку та захисту інформації України : Закон

України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet;

медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

1. Розлянемо основні поняття. Предмет, об'єкт і суб'єкти інформаційної безпеки.

Предметом інформаційних відносин є інформація та інформаційні ресурси в різних видах і формах, що захищається.

Об'єктами інформаційної безпеки можуть бути: свідомість, психіка людини, інформаційні системи різного масштабу і різного призначення.

Соціальними об'єктами інформаційної безпеки є особистість, колектив, суспільство, держава, світове товариство.

До *суб'єктів інформаційної безпеки* відносяться:

− держава, яка здійснює свої функції через відповідні органи;

− громадяни, суспільні та організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

1. Види інформаційної безпеки

Інформаційна безпека особистості – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства , образ тощо.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних видів життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т.ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси тощо) інформаційних впливів, причому як з упровадження, так і добування інформації.

Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

2. Концепція інформаційної безпеки держави

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення.

В концепції інформаційної безпеки держави:

– проводяться системна класифікація дестабілізуючих факторів і інформаційних загроз безпеці особливості ,суспільства і держави;

– обґрунтовуються основні положення організації забезпечення інформаційної безпеки держави;

– розробляються пропозиції по способах і формах забезпечення інформаційної безпеки.

У зв'язку з рішенням Ради національної безпеки і оборони України від 21.03.2008 р. «Про невідкладні заходи щодо забезпечення інформаційної безпеки України», введеним у дію Указом Президента України від 23.04.2008 р. № 377, було затверджено *Доктрину інформаційної безпеки України* (Указ Президента України від 08.07.2009 р. № 514/2009).

У Доктрині наголошується, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

3. Державна таємниця як особливий вид інформації, що захищається

Закон України «Про державну таємницю» від 21 січня 1994 р., № 3855-XII регулює суспільні відносини, пов'язані з віднесенням певних відомостей до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці в інтересах національної безпеки України.

Державна таємниця (секретна інформація) – вид таємної інформації, що охоплює відповідні відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені в порядку, встановленому цим законом, державною таємницею і підлягають охороні державою.

Віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з визначенням можливої шкоди національній безпеці України в разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього.

Допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації.

Доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

Звід відомостей, що становлять державну таємницю, – акт, у якому зведено переліки відомостей, що згідно з рішенням державних експертів із питань таємниць становлять державну таємницю у визначених цим Законом сферах.

Категорія режиму секретності – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю і зосереджені в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях.

II. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 3. Правові питання захисту інформації з використанням технічних засобів
Практичне заняття № 3. Правові питання захисту інформації з використанням технічних засобів.
Навчальна мета заняття: розглянути поняття про особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації.
Кількість годин: 2 год.
Навчальні питання:

1. Особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації та при розробці шифрувальних засобів.
2. Правове регулювання захисту інформації в засобах зв'язку.
3. Правове регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК,

2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

1. Розглянемо основні поняття про особливості правового регулювання суспільних відносин при використанні технічних засобів обробки інформації та при розробці шифрувальних засобів.

Правову основу технічного захисту інформації в Україні становлять Конституція України, закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України з питань технічного захисту інформації, згода на обов'язковість яких надана Верховною Радою України, а також Положення про технічний захист інформації в Україні.

Технічний захист інформації (ТЗІ) – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Система ТЗІ – це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база. *Комплекс технічного захисту інформації* – це сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

Основними напрямами державної політики у сфері ТЗІ є:

1) нормативно-правове забезпечення;

2) організаційне забезпечення;

3) науково-технічна та виробнича діяльність.

Рівень безпеки інформації, що обробляється в системах та на об'єктах інформаційної інфраструктури, визначається такими властивостями:

– *конфіденційність* – властивість інформації бути захищеною від несанкціонованого ознайомлення;

– *цілісність* – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

– *доступність* – властивість інформації бути захищеною від несанкціонованого блокування.

Основними нормативними актами, що регулюють використання криптографії в Україні, є закони «Про інформацію», «Про науково-технічну інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 р. № 2919-III.

Криптографічний захист інформації – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Засоби криптографічного захисту інформації без уведених ключових даних мають *гриф обмеження доступу*, який відповідає грифу обмеження доступу опису криптосхеми. Гриф обмеження доступу ключових документів, що використовуються для криптографічного захисту інформації, повинен відповідати грифу обмеження доступу інформації, що захищається.

2. Правове регулювання захисту інформації в засобах зв'язку

Сфера телекомунікацій є складовою частиною галузі зв'язку України. Закон України «Про телекомунікації» від 18 листоп. 2003 р. № 1280-IV визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами.[1]

Метою регулювання у сфері телекомунікацій є максимальне задоволення попиту споживачів на телекомунікаційні послуги, створення сприятливих організаційних та економічних умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних мереж з урахуванням інтересів національної безпеки.

Надання телекомунікаційних послуг на території України є виключним правом юридичних осіб з місцезнаходженням на території України, які зареєстровані відповідно до законодавства України, та/або фізичних осіб – суб'єктів підприємницької діяльності з постійним місцем проживання на території України.

Закон України «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 р. № 2919-III зазначає, що *Національна система конфіденційного зв'язку* сукупність

[1]Телекомунікації (електрозв'язок) – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах.

спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану.

Суб'єкти Національної системи конфіденційного зв'язку – органи державної влади та органи місцевого самоврядування, юридичні та фізичні особи, що беруть участь у створенні, функціонуванні, розвитку та використанні цієї системи.

Складовими Національної системи конфіденційного зв'язку є спеціальні телекомунікаційні системи (мережі), їх фіксовані і мобільні компоненти, централізовані системи захисту інформації та оперативно-технічного управління. (Частина друга статті 5 із змінами, внесеними згідно із Законом N 2599-IV від 31.05.2005)

Структура побудови Національної системи конфіденційного зв'язку повинна забезпечувати відокремлення конфіденційної інформації органів державної влади та органів місцевого самоврядування, інших юридичних та фізичних осіб з використанням криптографічних та/або технічних засобів.

3. Правове регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу

3. Правове регулювання використання цифрового підпису і захисту інформації в системах і засобах електронного документообігу

07.11.2018 набув чинності Закон України «Про електронні довірчі послуги» від 05.10.2017 р. №2155-VIII (далі – Закон №2155).

Одним з найважливіших положень Закону № 2155 є взаємне визнання українських та іноземних сертифікатів відкритих ключів та **електронних підписів**.

Законом запроваджуються такі механізми, як електронна ідентифікація, електронний підпис, електронна печатка, електронна позначка часу, реєстрована електронна доставка, інтероперабельність тощо.

Згідно з ч.2 ст. 22 Закону № 2155 **ідентифікація** фізичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи..

Отже, починаючи з 07.11.2018, отримати послуги з формування кваліфікованих **сертифікатів відкритих ключів** за довіреністю (в т.ч. посвідченою нотаріально) буде неможливо. Про це зазначають податківці на сайті ДФСУ.

Крім того, запроваджується адміністративна послуга щодо включення юридичних та фізичних осіб - підприємців, які мають намір надавати електронні довірчі послуги (ЕДП), до Довірчого списку, а також встановлюється порядок ведення такого списку. Також, визначається процедура незалежної оцінки відповідності для ЕДП та також можливість використання зазначеними особами у своїй діяльності як національних, так і міжнародних стандартів.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 4. Загрози інформаційній безпеці, безпеці інформації та інформаційних ресурсів
Практичне заняття № 4. Загрози інформаційній безпеці.
Навчальна мета заняття: розглянути джерела загроз інформаційній безпеці. Методи і засоби забезпечення інформаційної безпеки: основні принципи, система забезпечення, основні фактори і способи.
Кількість годин: 1год.
Навчальні питання:

1. Класифікація загроз інформаційній безпеці.
2. Ієрархічна класифікація загроз інформаційній безпеці.
3. Джерела загроз інформаційній безпеці.
4. Методи і засоби забезпечення інформаційної безпеки: основні принципи, система забезпечення, основні фактори і способи.

Література:
Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.

12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

1. Розглянемо основні поняття як :класифікація загроз інформаційній безпеці

Основні *загрози інформаційній безпеці* можна розділити на три групи:

– загрози впливу неякісної інформації;

– загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси;

– загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т.ін.).

Існують три основні типи загроз безпеці інформації: конфіденційності, доступності, цілісності.

Загрози при забезпечення *конфіденційності*:

– крадіжка (копіювання) інформації та засобів обробки;

– втрата (витік) інформації та засобів обробки;

Загрози безпеці інформації при забезпеченні *доступності*:

– блокування інформації;

– знищенні інформації та засобів її обробки.

Загрози безпеці інформації при забезпеченні *цілісності*:

– модифікація (спотворення) інформації;

– заперечення автентичності інформації;

– нав'язування фальшивої інформації.

2. Ієрархічна класифікація загроз інформаційній безпеці

Глобальні фактори загроз інформаційній безпеці:

– недружня політика іноземних держав у галузі глобального інформаційного моніторингу;

– діяльність іноземних розвідувальних та спеціальних служб;

– діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;

– злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

– невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;

– недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;

– розвиток зарубіжних технічних засобів розвідки, та промислового шпіонажу, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;

– зростання злочинності в інформаційній сфері;

– відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:

– перехоплення електронних випромінювань;

– застосування підслуховуючих пристроїв або закладок;

– дистанційне фотографування;

– розкрадання носіїв інформації та промислових відходів;

– копіювання носіїв інформації з подоланням заходів захисту;

– незаконне приєднання до апаратури та ліній зв'язку;

– упровадження та використання комп'ютерних вірусів тощо.

3. Джерела загроз інформаційній безпеці

Усі джерела загроз безпеці інформації можна розділити на три групи:

– обумовлені діями суб'єкта (антропогенні джерела загроз);

– обумовленні технічними засобами (техногенні джерела загроз);

– обумовлені стихійними джерелами.

Антропогенними джерелами загроз є суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини:

– суб'єкти, які мають доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що підлягає захисту;

– суб'єкти, дії яких можуть призвести до порушення безпеки інформації (зовнішні та внутрішні).

Друга група включає джерела загроз, що визначаються *технократичною* діяльністю людини і розвитком цивілізації і є особливо актуальними у сучасних умовах. Технічні засоби, котрі є джерелами потенційних загроз безпеці інформації можуть бути зовнішніми і внутрішніми.

Третя група джерел загроз об'єднує обставини, що складають непереборну силу і носять об'єктивний і абсолютний характер. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або запобігти при сучасному рівні знань і можливостей людини.

4. Методи і засоби забезпечення інформаційної безпеки: основні принципи, система забезпечення, основні фактори і способи

В основу забезпечення інформаційної безпеки держави покладені наступні принципи:

– законність, дотримання балансу інтересів особистості, суспільства і держави;

– взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

– інтеграція систем національної і міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:

– превентивний характер проведення її заходів по відношенню до заходів інших видів безпеки;

– адекватна інформованість об'єктів безпеки, в тому числі і міжнародних.

В основі прав і свобод держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, екології, оборони і т.ін. лежать діючі норми та принципи міждержавного права. Головним вважається *принцип рівної безпеки.* Стосовно до інформаційної сфери можна говорити про його трансформацію в *принцип адекватної інформованості держав світового співтовариства***,** який передбачає право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки усіх членів співтовариства в рівній мірі, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі.

Система забезпечення інформаційної безпеки держави представляє організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Основними завданнями такої системи є:

– виявлення і прогнозування дестабілізуючих факторів і інформаційних загроз інформаційних життєво важливим інтересам особистості, суспільства та держави;

– здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;

– створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, через який сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 4: Загрози інформаційній безпеці, безпеці інформації та інформаційних ресурсів
Практичне заняття № 4 :Загрози безпеці інформації та інформаційних ресурсів.
Навчальна мета заняття: розглянути джерела загроз інформаційній безпеці.
Кількість годин: 1 год.
Навчальні питання:

1. Класифікація джерел загроз.
2. Ранжування джерел загроз безпеці інформації. Методи ранжування загроз безпеці інформації.
3. Класифікація та ранжування уразливостей безпеці інформації.
4. Класифікація актуальних загроз безпеці інформації.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо основні поняття про класифікацію джерел загроз. Джерелами загроз можуть бути як суб'єкти, так і об'єктивні прояви. Джерела загроз можуть бути як в середині організації – внутрішні джерела, так і ззовні її – зовнішні джерела.

Усі джерела загроз безпеці інформації можна розділити на три групи:

– обумовлені діями суб'єкта (антропогенні джерела загроз);

– обумовленні технічними засобами (техногенні джерела загроз);

– обумовлені стихійними джерелами.

Антропогенними джерелами загроз є суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини:

– суб'єкти, які мають доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що підлягає захисту;

– суб'єкти, дії яких можуть призвести до порушення безпеки інформації (зовнішні та внутрішні).

Друга група включає джерела загроз, що визначаються *технократичною* діяльністю людини і розвитком цивілізації і є особливо актуальними у сучасних умовах. Технічні засоби, котрі є джерелами потенційних загроз безпеці інформації можуть бути зовнішніми і внутрішніми.

Третя група джерел загроз об'єднує обставини, що складають непереборну силу і носять об'єктивний і абсолютний характер. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або запобігти при сучасному рівні знань і можливостей людини.

2. Ранжирування джерел загроз безпеці інформації. Методи ранжирування загроз безпеці інформації

Усі джерела загроз мають різну *міру небезпеки,* яку можна оцінити, якщо провести їхнє ранжирування. Критеріями порівняння (показників) пропонується, наприклад, вибрати:

– *можливість виникнення джерела* – визначає міру доступності до можливості використати фактор (уразливість) (для антропогенних джерел), віддаленість від фактора (уразливості) (для техногенних джерел) або особливості обстановки (для випадкових джерел);

– *готовність джерела* що визначає міру кваліфікації та привабливість здійснення діяння зі сторони джерела загрози (для антропогенних джерел) або наявність необхідних умов (для техногенних та стихійних джерел).

– *фатальність* – визначає міру непереборності наслідків реалізації загрози.

Міра доступності до об'єкта, що підлягає захисту, може бути класифікована за наступною шкалою:

– висока ступінь доступності – антропогенне джерело загроз має повний доступ до технічних і програмних засобів обробки інформації, що підлягає захисту;

– перша середня ступінь доступності – антропогенне джерело загроз має можливість опосередкованого, не визначеного функціональними обов'язками, доступу до технічних і програмних засобів обробки інформації, що підлягає захисту (характерно);

– друга середня ступінь доступності – антропогенне джерело загроз має обмежену можливість до програмних засобів у силу введених обмежень при використанні технічних засобів, функціональних обов'язків або за видом своєї діяльності;

– низька ступінь доступності – антропогенне джерело загроз має дуже обмежену можливість доступу до технічних засобів і програм, які обробляють інформацію, що підлягає захисту;

– відсутність доступності – антропогенне джерело загроз не має доступу до технічних засобів і програм, які обробляють інформацію, що підлягає захисту.

Міра непереборності наслідків загрози (фатальність) визначається за наступною шкалою:

– неперебoрні наслідки – результати прояву загрози можуть призвести до повного руйнування (знищення, втрати) об'єкта захисту і, як наслідок, до непоправних втрат і виключення можливості доступу до інформаційних ресурсів, що підлягають захисту;

– практично неперебoрні наслідки – результати прояву загрози можуть призвести до руйнування (знищення, втрати) об'єкта та до значних витрат (матеріальних, часу і т.ін.) на відновлення, які порівнянні з витратами на створення нового об'єкта та суттєвого обмеження часу доступу до інформаційних ресурсів, що підлягають захисту;

– частково переборні наслідки – результати прояву загрози можуть призвести до часткового руйнування і, як наслідок, до значних витрат на відновлення, обмеження часу доступу до інформаційних ресурсів, що підлягають захисту;

– переборні наслідки – результати прояву загрози можуть призвести до часткового руйнування (знищення, втрати) об'єкта захисту, що не потребує великих витрат на його відновлення і, практично не впливає на обмеження часу доступу до інформаційних ресурсів, які підлягають захисту;

– відсутність наслідків – результати прояву загрози не можуть уплинути на діяльність об'єкта захисту.

3. Класифікація та ранжирування уразливостей безпеці інформації

Об'єктивні уразливості залежать від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту. Повне усунення цих уразливостей неможливе, але вони можуть суттєво послаблятися технічними та інженерно-технічними методами відбивання загроз безпеці інформації.

Суб'єктивні уразливості залежать від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами.

Випадкові уразливості залежать від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин. Ці фактори, як правило, мало передбачувані і їх усунення можливе тільки при проведенні комплексу організаційних та інженерно-технічних заходів із протидії загрозам інформаційній безпеці.

Усі уразливості мають різну міру небезпеки, яку можна кількісно оцінити на основі ранжирування. При цьому критеріями порівняння (показниками) можна вибрати:

– фатальність – визначає міру впливу уразливості на непереборність наслідків реалізації загрози. Для об'єктивних уразливостей – це інформативність, тобто здатність

уразливості повністю (без спотворення) передати корисний інформаційний сигнал;

– доступність – визначає зручність (можливість) використання уразливості джерелом загроз (масогабаритні розміри, складність, вартість необхідних засобів, можливість використання не спеціалізованої апаратури);

– кількість – визначає кількість елементів об'єкта, яким характерна та чи інша уразливість.

4. Класифікація актуальних загроз

При проведенні актуальних загроз експертно-аналітичним методом визначаються об'єкти захисту, що піддаються впливу цієї чи іншої загрози, характерні джерела цих загроз і уразливості, що сприяють реалізації загроз.

На основі аналізу складається таблиця взаємозв'язку джерел загроз і уразливостей, із яких визначаються можливі наслідки реалізації загроз (атаки) та обчислюється коефіцієнт небезпеки цих атак як добуток коефіцієнтів небезпеки відповідних загроз та джерел загроз, визначених раніше. При цьому передбачається, що атаки, які мають коефіцієнт небезпеки менше 0,1 (припущення експертів), в подальшому можуть не розглядатися із-за малої ймовірності їх здійснення на об'єкті захисту.

Така матриця складається окремо для кожної загрози. І вже після виявлення найбільш актуальних загроз приймаються заходи з вибору методів і засобів для відбивання.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 5. Юридична відповідальність за порушення правових норм в галузі інформаційної безпеки

Практичне заняття. Сучасні основи інформаційної безпеки України

Навчальна мета заняття: розглянути поняття і види юридичної відповідальності за порушення правових норм в сфері інформаційної безпеки. Особливості юридичної відповідальності за порушення правових норм інформаційної безпеки в галузі трудових норм і цивільно-правових відносин.

Кількість годин: 2 год.

Навчальні питання:

1. Поняття і види юридичної відповідальності за порушення правових норм в сфері інформаційної безпеки.
2. Кримінальна відповідальність за порушення правових норм в сфері інформаційної безпеки.
3. Адміністративна відповідальність за порушення правових норм в сфері інформаційної безпеки.
4. Особливості юридичної відповідальності за порушення правових норм інформаційної безпеки в галузі трудових норм і цивільно-правових відносин.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125

«Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL:

https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо основні поняття як: поняття та види юридичної відповідальності за порушення правових норм в сфері інформаційної безпеки.

Юридична відповідальність розуміється як зобов'язання особи зазнавати певні незручності держано-власного характеру, які передбачені законом за вчинені протиправні дії. Найбільш розповсюджена класифікація юридичної відповідальності за галузевою належністю. Види юридичної відповідальності співпадають з видами правопорушень.

Зазначені види правопорушень і юридична відповідальність є характерними і для галузі інформаційної безпеки – для захисту конфіденційної інформації, що обробляється в АСОД (автоматизовані системи обробки даних). Відповідно, у зв'язку із глобальною комп'ютеризацією інформаційних процесів особливу увагу необхідно приділяти правопорушенням стосовно конфіденційної інформації, яка обробляється в АСОД.

При визначенні характеристик правопорушень інформаційної безпеки враховуються:

– властивості правопорушень, що розглядаються;

– залежність діянь від об'єктивних і суб'єктивних ознак злочинів ,що вчиняються в сфері інформаційної безпеки;

– ситуаційна безпека вчинення правопорушень інформаційної безпеки;

– залежність вирішення завдань попередження правопорушень інформаційної безпеки від заходів правового регулювання діяльності в різних сферах (економіки, зовнішньої політики, воєнній сфері тощо);

– наявність різних форм власності та ін..

1. Кримінальна відповідальність за порушення правових норм в сфері інформаційної безпеки

Розгляд ознак правопорушень інформаційної безпеки здійснюється з врахуванням кримінальної і адміністративної характеристик.

Кримінально-правові норми, спрямовані на захист державної таємниці, містяться у розд. I «Злочини проти основ національної безпеки України», до якого включені ст. 111 «Державна зрада» та ст. 114 «Шпигунство», а також у розд. XIV «Злочини у сфері охорони державної таємниці, недоторканності кордонів, забезпечення призову та мобілізації», до якого входять ст. 328 «Розголошення державної таємниці» і ст. 329 «Втрата документів, що містять державну таємницю».

Винні в розголошенні даних досудового слідства несуть кримінальну відповідальність за ст. 387 КК України.

Кримінальним кодексом передбачена відповідальність за злочинні дії, що пов'язані з порушенням вимог охорони комерційної таємниці: незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231), розголошення комерційної або банківської таємниці (ст. 232). Кримінальна відповідальність визначається ст. 132 «Розголошення відомостей про проведення медичного огляду на виявлення зараженням вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби», ст. 140 «Неналежне виконання професійних обов'язків медичним або фармацевтичним працівником», ст. 145 «Незаконне розголошення лікарської таємниці».

Адвокати, винні в розголошенні конфіденційних відомостей, що становлять

адвокатську таємницю, несуть дисциплінарну відповідальність, а в разі розголошення ними без дозволу слідчого або прокурора даних попереднього слідства – і кримінальну відповідальність (ст. 387 КК України).

У ст. 80 «Основ законодавства України про охорону здоров'я» вказується, що особи, винні в порушенні законодавства про охорону здоров'я, несуть кримінальну, цивільну або адміністративну відповідальність згідно із законодавством. Особи, винні у порушенні законодавства про психіатричну допомогу, несуть відповідальність згідно з законами України (ст. 33 Закону України «Про психіатричну допомогу»).

2. Адміністративна відповідальність за порушення правових норм в сфері інформаційної безпеки

Кодекс України про адміністративні правопорушення (далі – КУпАП) передбачає адміністративну відповідальність за порушення законодавства про державну таємницю (ст. 212–2).

Кримінально-процесуальний кодекс відносить зазначені вище злочини до підслідності Служби безпеки України.

Адміністративна відповідальність за порушення, що пов'язані з комерційною таємницею, встановлюється за отримання, використання, розголошення комерційної таємниці ст. 164-3 КУпАП.

3. Особливості юридичної відповідальності за порушення правових норм інформаційної безпеки в сфері цивільно-правових відносин і трудових норм

Законом України «Про захист від недобросовісної конкуренції» від 7 червня 1996 р. № 236/96-ВР передбачена відповідальність: статтями 16, 17,18,19.

Правові гарантії захисту особистої інформації встановлені ЦК України: ч. 3 ст. 277, ст. 278, ч. 4 ст. 296, ст. 302.

Використання комп'ютерної програми без відповідного дозволу (ліцензії) автора, невиконання умов договору є порушенням авторських прав і може бути підставою для притягнення особи-порушника до наступних видів відповідальності згідно з чинним законодавством України: цивільно-правової (майнової) – ст. 431 ЦК та ст. 52 Закону України «Про авторське право і суміжні права»; кримінальної – ст. 176 КК України.

У зв'язку із цим до КУпАП були внесені зміни: спочатку включено ст. 51-2, якою передбачено відповідальність за порушення права на об'єкт права інтелектуальної власності, а потім ст. 164-9, якою передбачено відповідальність за незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних.

Використання комп'ютерної програми без відповідного дозволу (ліцензії) автора, невиконання умов договору є порушенням авторських прав і може бути підставою для притягнення особи-порушника до наступних видів відповідальності згідно з чинним законодавством України:

– цивільно-правової (майнової) – ст. 431 ЦК та ст. 52 Закону України «Про авторське право і суміжні права»;
– адміністративної – ст. 51-2 КУпАП;
– кримінальної – ст. 176 КК України.

Під час розгляду справ про правопорушення у сфері інтелектуальної власності судді, вирішуючи питання про притягнення правопорушника до адміністративної відповідальності та накладення адміністративного стягнення, мають одночасно вирішувати й питання про відшкодування винним майнової шкоди за завдані суб'єкту права протиправними діями збитки. Стаття 431 ЦК встановлює, що порушення права інтелектуальної власності, у тому числі невизнання цього права чи посягання на нього, тягне за собою відповідальність, встановлену цим Кодексом, іншим законом чи договором.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач

також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 6: Загальна характеристика каналів витоку інформації
Практичне заняття: Загальна характеристика каналів витоку інформації.
Навчальна мета заняття: розглянути поняття та класифікацію технічних каналів витоку інформації (ТКВІ).
Кількість годин: 2 год.
Навчальні питання:

1. Технічні канали витоку інформації.
2. Поняття та класифікація технічних каналів витоку інформації (ТКВІ).
3. Акустичні канали витоку інформації.
4. Канали витоку інформації за рахунок побічних електромагнітних випромінювань і наведень ((ПЕМВН) засобів електронно-обчислювальної техніки.

Література:
Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК,

2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо основні поняття як : технічні канали витоку інформації.

Фізичні процеси, що відбуваються в технічних засобах і системах, призначених для приймання, передавання, оброблення і зберігання інформації при їх функціонуванні, створюють в навколишньому середовищі побічні електромагнітні, акустичні та інші випромінювання, котрі можуть виявлятися на досить значних відстанях (до сотень метрів) і використовуватися зловмисниками, які намагаються отримати доступ до секретної інформації.

Побічні електромагнітні випромінювання виникають унаслідок непередбаченою схемою або конструкцією даного технічного засобу передачі інформації по паразитних зв'язках напруги, струму, заряду або магнітного поля.

Джерелами випромінювань в технічних каналах є різноманітні технічні засоби, в яких циркулює інформація з обмеженим доступом. Такими засобами можуть бути:

- мережі електроживлення та лінії заземлення;
- автоматичні мережі телефонного зв'язку;
- системи телеграфного, телекодового і факсимільного зв'язку;
- засоби гучномовного зв'язку;
- засоби звуко- і відеозаписе;

– системи звукопідсилення мови;
– електронно-обчислювальна техніка;
– електронні засоби оргтехніки.

2. Поняття та класифікація причин утворення технічних каналів витоку інформації

Технічні канали витоку інформації прийнято ділити на такі типи:
– радіоканали (електромагнітні випромінювання радіодіапазону);
– акустичні канали (розповсюдження звукових коливань в будь-якому звукопровідному матеріалі);
– електричні канали (небезпечна напруга і струми в струмопровідних комунікаціях);
– оптичні канали (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій частині спектру);
– матеріально-речові канали (папір, фото, магнітні носії, відходи і т. д).

Утворенню технічних каналів витоку інформації сприяють певні обставини і причини технічного характеру:
– недосконаліть елементної бази і схемних рішень, прийнятих для даної категорії технічних засобів (конструкторських, технологічних);
– експлуатаційний знос елементів виробу (зміна характеристик, аварійний вихід з ладу);
– зловмисні дії (підміна характеристик, створення аварійних ситуацій, блокування засобів захисту).

Основними *джерелами утворення технічних каналів витоку інформації* є:
– акустичні перетворювачі: індуктивні, ємкісні, п'єзоелектричні, оптичні);
– випромінювачі електромагнітних коливань: низькочастотні, високочастотні, оптичні;
– паразитні зв'язки і наведення на дроти та елементи електронних пристроїв: зворотний зв'язок, по ланцюгах живлення, по ланцюгах заземлення.

Технічні засоби і системи можуть:
– безпосередньо випромінювати в простір сигнали, що містять оброблювану ними інформацію;
– уловлювати за рахунок своїх мікрофонних або антенних властивостей, що існують в безпосередній близькості від них, акустичні або електромагнітні випромінювання.

3. Акустичні канали витоку інформації

Класифікація акустичних каналів витоку інформації базується на основних визначеннях акустики.[2]

Класифікація акустичних каналів витоку інформації може бути:
– за природою утворення: мова, шуми, промислові коливання;
– по середовищу розповсюдження: повітряний простір, тверде середовище, водяне середовище;[3]

---

[2] *Звуком* називаються механічні коливання частинок пружного середовища (повітря, води, металу і так далі), які суб'єктивно сприймаються органом слуху. Звукові відчуття викликаються коливаннями середовища, що відбуваються в діапазоні частот від 16 до 20000 Гц.
Гучність звуку – інтенсивність звукового відчуття, викликана даним звуком у людини з нормальним слухом. Гучність залежить від сили звуку і його частоти, вимірюється пропорційно логарифму сили звуку і виражається кількістю децибел, на яку даний звук перевищує по інтенсивності звук, прийнятий за поріг чутності. Одиниця вимірювання гучності – фон.
Динамічний діапазон – діапазон гучності звуку або різниця рівнів звукового тиску найгучнішого і найтихішого звуків, виражена в децибелах.
Джерелом утворення акустичного каналу витоку інформації є вібруючі тіла і механізми, що коливаються, такі як голосові зв'язки людини, рухомі елементи машин, телефонні апарати, звукопідсилювачі тощо.
[3] Розповсюдження звуку в просторі здійснюється звуковими *пружними* або *механічними* хвилями. *Хвилями* називаються механічні обурення (деформації), що розповсюджуються в пружному середовищі. Тіла, які,

– по діапазону: інфразвук, гучний звук (голос людини), ультразвук.

Акустичні канали витоку інформації утворюються за рахунок:

– розповсюдження механічних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті вікна, двері, хвіртки, вентиляційні канали);

– впливу звукових коливань на елементи і конструкції будівель, що викликають їх вібрацію (стіни, стеля, підлога, вікна, двері, короби вентиляційних систем, труби водопостачання, опалення тощо;

– впливу звукових коливань на технічні засоби обробки інформації (мікрофонний ефект, акустична модуляція, волоконно-оптичні лінії передачі інформації.

Отже, під *акустичною розуміється інформація, носієм якої є акустичні сигнали.* Залежно від фізичної природи виникнення інформаційних сигналів, середовища розповсюдження акустичних коливань і способів їх перехоплення, акустичні канали витоку інформації можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронні і параметричні.

Повітряні канали. У повітряних каналах витоку інформації середовищем, розповсюдження акустичних сигналів є повітря, а для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні направлені мікрофони. Мікрофони об'єднуються або з'єднуються з портативними звукозаписуючими пристроями (диктофонами) або спеціальними мініатюрними передавачами.

Вібраційні канали. У вібраційних (структурних) каналах витоку інформації середовищем розповсюдження акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалювання, каналізації і інші тверді тіла. Для перехоплення акустичних коливань в цьому випадку використовуються контактні мікрофони(стетоскопи).

Електроакустичні канали. Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні. Перехоплення акустичних коливань здійснюється через ВТСС, що володіють «мікрофонним ефектом», а також шляхом «високочастотного нав'язування».

Оптико-электронный канал. Оптико-электронный (лазерний) канал витоку інформації утворюється при опромінюванні лазерним променем вібруючих в акустичному полі тонких відзеркалювальних поверхонь (стекол, вікон, картин, дзеркал тощо).

Параметричні канали. В результаті дії акустичного поля міняється тиск на всі елементи високочастотних генераторів ТСПІ і ВТСС.

4. Канали витоку інформації за рахунок побічних електромагнітних випромінювань і наведень ((ПЕМВН) засобів електронно-обчислювальної техніки

Сучасні ПЕВМ можуть працювати як незалежно один від одного, так і взаємодіючи з іншими ЕОМ по комп'ютерних мережах, причому останні можуть бути не тільки локальними, але і глобальними. Відповідно, повний перелік тих ділянок, в яких можуть знаходитися що підлягають захисту дані, може мати наступний вигляд:

– безпосередньо у оперативній або постійній пам'яті ПЕВМ;

– на знімних магнітних, магнітооптичних, лазерних і інших носіях;

– на зовнішніх пристроях зберігання інформації колективного доступу (RAID-масиви, файлові сервери і тому подібне);

– на екранах пристроїв відображення (дисплеї, монітори, консолі);

– у пам'яті пристроїв введення/виводу (принтери, графічні пристрої, сканери);

– у пам'яті пристроїв, що управляють, і лініях зв'язку, утворюючих канали сполучення комп'ютерних мереж.

Канали витоку інформації утворюються як при роботі ПЕОМ, так і в режимі

впливаючи на середовище, викликають ці обурення, називаються *джерелами хвиль.*
Пружна хвиля є подовжньою і пов'язана з об'ємною деформацією пружного середовища, унаслідок чого може розповсюджуватися в будь-якому середовищі – твердому, рідкому і газоподібному.

очікування. Джерелами таких каналів є:

– електромагнітні поля;

– струми, що наводяться, і напруга в дротяних системах (живлення, заземлення і сполучних);

– перевипромінювання інформації, що обробляється, на частотах паразитної генерації елементів і пристроїв технічних засобів ПЕОМ;

– перевипромінювання оброблюваної інформації, на частотах контрольно-вимірювальної апаратури.

Передбачається три типи обробки: людиною, апаратурою, програмою. Відповідно до кожного типу обробки канали витоку також розбиваються на три групи.

Стосовно ПЕВМ групу каналів, в яких основним видом обробки є *обробка інформації людиною*, складають наступні можливі канали витоку:

– розкрадання матеріальних носіїв інформації (магнітних дисків, стрічок, карт);

– читання інформації з екрану сторонньою особою;

– читання інформації із залишених без нагляду паперових роздруківок.

У групі каналів, в яких основним видом обробки є *обробка інформації апаратурою,* можна виділити наступні можливі канали витоку:

– підключення до ПЕВМ спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

– використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань технічних засобів ПЕВМ.

У групі каналів, в яких основним видом *обробки інформації є програмна обробка*, можна виділити наступні можливі канали витоку:

– несанкціонований доступ програми до інформації;

– розшифровка програмою зашифрованої інформації;

– копіювання програмою інформації з носіїв;

– блокування або відключення програмних засобів захисту.

Класифікації радіоканалів витоку інформації

Аналіз фізичної природи численних перетворювачів і випромінювачів показує, що:

– джерелами небезпечного сигналу є елементи, вузли і провідники технічних засобів забезпечення виробничої і трудової діяльності, а також радіо- і електронна апаратура;

– кожне джерело небезпечного сигналу за певних умов може утворити технічний канал просочування інформації;

– кожна електронна система, що містить в собі сукупність елементів, вузлів і провідників, володіє деяким безліччю технічних каналів просочування інформації.

Кожен з цих каналів, залежно від конкретної реалізації елементів, вузлів і виробів в цілому, матиме певний прояв, специфічні характеристики і особливості утворення, пов'язані з умовами розташування і виконання. Радіоканали витоку інформації утворюються внаслідок:

– мікрофонного ефекту;

– магнітного поля;

– паразитної генерації;

– ланцюгом живлення;

– ланцюгом заземлення;

– взаємного впливу;

– електромагнітного випромінювання;

– із волоконно-оптичних систем зв’язку;

– нав’язування потужних радіо засобів.

Класифікація радіоканалів витоку інформації за природою утворення діапазону випромінювання і середовищу розповсюдження така:

за природою утворення – електромагнітне випромінювання, паразитні зв’язки і наведення акустоперетворювальні;

по діапазону випромінювання – наддовгі хвиля, довгі хвилі ,середні хвилі, короткі хвилі, ультракороткі хвилі;

по середовищу розповсюдження – безповітряний простір, повітряний простір, ґрунтове середовище, водяне середовище, направлені системи.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 7. Функціональні вимоги до засобів захисту

Практичне заняття № 7. Критерії безпеки інформаційних технологій

Навчальна мета заняття: розглянути основні положення критеріїв загальних критеріїв безпеки інформаційних технологій.

Кількість годин: 2 год.

Навчальні питання:

1. Поняття про стандарти інформаційної безпеки.
2. Критерії безпеки комп'ютерних систем.
3. Європейські критерії безпеки інформаційних технологій.
4. Основні Федеральні критерії інформаційних технологій.
5. Канадські критерії інформаційних технологій.
6. Основні положення критеріїв загальних критеріїв безпеки інформаційних технологій.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з

дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо основні критерії безпеки інформаційних технологій та основні поняття про стандарти інформаційної безпеки.

Стандарти інформаційної безпеки — це стандарти забезпечення захисту, призначені для взаємодії між виробниками, споживачами і експертами з кваліфікації продуктів інформаційних технологій у процесі створення та експлуатації захищених систем оброблення інформації.

Стандарт забезпечення захисту звичайно містять опис послідовності оцінок, які необхідно виконати, щоб вважати дану характеристику безпеки підтвердженою з точки зору атестації захисту або множину характеристик безпеки, які повинна забезпечити система захисту, щоб її можна було використовувати в даному конкретному режимі забезпечення

безпеки або у відповідності до загальної стратегії захисту.

1. Критерії безпеки комп'ютерних систем – стандарт інформаційної безпеки, розроблений міністерством оборони США у 1983 р. з метою визначення вимог безпеки, що пред'являються до апаратного, програмного і спеціального забезпечення комп'ютерних систем і вироблення відповідної методології аналізу політики безпеки, що реалізується в комп'ютерних системах воєнного призначення. У критеріях пропонуються три категорії вимог безпеки – політика безпеки, аудит і коректність, в рамках яких сформульовані шість базових вимог безпеки:

– політика безпеки, мітки — в рамках політики безпеки;

– ідентифікація та автентифікація, реєстрація та облік – в рамках аудиту;

– контроль коректності функціонування засобів захисту, безперервність захисту – в рамках коректності.

Перші чотири вимоги спрямовані безпосередньо на забезпечення безпеки інформації, а дві останні – на якість самих засобів захисту.

2. Європейські критерії безпеки інформаційних технологій розглядають наступні завдання засобів інформаційної безпеки:

– захист інформації від несанкціонованого доступу для забезпечення конфіденційності;

– забезпечення цілісності інформації за допомогою захисту її від несанкціонованої модифікації або знищення;

– забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Рівні безпеки в «Європейських критеріях» – рівні для визначення ступеню безпеки системи. В «Європейських критеріях» визначені три рівні безпеки – базовий, середній і високий.

«Європейські критерії» покладені в основу багатьох стандартів безпеки комп'ютерних систем. На основі цих критеріїв Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України розроблені нормативні документи системи технічного захисту інформації України стосовно технічного захисту інформації на програмно-керованих АТС загального користування.

3. Федеральні критерії безпеки інформаційних технологій – стандарт інформаційної безпеки, розроблений Національним інститутом стандартів і технологій США (NIST) і Агентством національної безпеки США (NSA) у 90-х роках для використання в Американському федеральному стандарті з оброблення інформації.

«Федеральні критерії» охоплюють практично весь спектр проблем, зв'язаних із захистом та забезпеченням безпеки, так як включають усі аспекти конфіденційності, цілісності та працездатності. Основними об'єктами застосування вимог безпеки критеріїв є продукти інформаційних технологій (ІТ-продукти) і системи оброблення інформації. Ключовим поняттям концепції інформаційної безпеки «Федеральних критеріїв» є поняття профілю захисту.

Відповідно до «Федеральних критеріїв» процес розробки систем оброблення інформації здійснюється у вигляді послідовності наступних основних етапів:

– розроблення та аналіз профілю захисту;

– розроблення і кваліфікаційний аналіз ІТ-продуктів;

– компонування та сертифікація системи оброблення інформації.

Процес створення ІТ-продуктів і компонування систем оброблення інформації залишаються за межами цього стандарту.

4. Канадські критерії безпеки комп'ютерних систем – національний стандарт інформаційної безпеки, розроблений Центром безпеки відомства безпеки зв'язку Канади.

«Канадські критерії» використовуються для розроблення вимог безпеки, специфікацій засобів захисту та сертифікації програмного забезпечення робочих станцій, багатопроцесорних обчислювальних систем, персональних і багатокористувальницьких операційних систем, систем керування базами даних, розподілених, мережних, вбудованих, проблемно-орієнтованих та інших систем.

В «Канадських критеріях» пропонується оригінальний підхід до опису взаємодії користувачів із комп'ютерною системою, інваріантний по відношенню до політики безпеки. Усі компоненти системи, які знаходяться під керуванням ядра безпеки, називаються об'єктами.

Об'єкти можуть знаходитися в одному з наступних трьох станів: *об'єкт-користувач, об'єкт-процес, пасивний об'єкт,* і в залежності від стану, позначають користувачів, процеси та об'єкти відповідно.

При описі критеріїв конфіденційності та цілісності (довільного та нормативного керування доступом і цілісністю) в «Канадських критеріях» використовується поняття тег.

Тега – сукупність атрибутів асоційованих із користувачем, процесом або проектом.

У критеріях застосований дуальний принцип подання вимог безпеки у вигляді функціональних вимог до засобів захисту та вимог до гарантій їхньої реалізації.

Канадські критерії безпеки комп'ютерних систем покладені в основу Критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, розроблених Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України для системи технічного захисту інформації України.

6. Загальні критерії безпеки інформаційних технологій – стандарт інформаційної безпеки, що узагальнює зміст і досвід використання «Жовтогарячої книги».

Матеріали стандарту – це вимоги і гарантії з інформаційної безпеки, які можуть відбиратися та реалізовуватися у функціональні стандарти (профілі захисту) забезпечення інформаційної безпеки для конкретних систем, мереж і засобів як користувачами (по відношенню до того, що вони хочуть одержати в продукті, який пропонується), так і розробниками й операторами мереж (по відношенню до того, що вони гарантують у продукті, який реалізується).

Основними компонентами безпеки «Загальних критеріїв» є:

– потенційні загрози безпеці та завдання захисту;

– політика безпеки; продукт інформаційних технологій;

– профіль захисту;

– проект захисту;

– функціональні вимоги безпеки;

– вимоги гарантій безпеки;

– рівні гарантій.

Стандарт «Загальних критеріїв» описує тільки загальну схему проведення кваліфікаційного аналізу та сертифікації, але не регламентує процедуру їх здійснення.

Кваліфікаційний аналіз – це аналіз обчислювальної системи з метою визначення рівня її захищеності та відповідності вимогам безпеки на основі критеріїв стандарту інформаційної безпеки.

Процес кваліфікаційного аналізу включає три стадії:

– аналіз профілю захисту на предмет його повноти, несуперечності, реалізованості та можливості використання у вигляді набору вимог для продукту, що аналізується;

– аналіз проекту захисту на предмет його відповідності вимогам профілю захисту, а також повноти, несуперечності, реалізованості і можливості використання у вигляді еталона при аналізі ІТ-продукту;

– аналіз ІТ-продукту на предмет відповідності проекту захисту. Результатом кваліфікаційного аналізу є висновок про те, що підданий аналізу ІТ-продукт відповідає представленому проекту захисту.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 8. Основи управління інформаційною безпекою
Практичне заняття: Загальна характеристика каналів витоку інформації.
Навчальна мета заняття: розглянути основні методи і засоби захисту інформації в комп'ютерних системах від випадкових загроз.
Кількість годин: 2 год.
Навчальні питання:

1. Загальна характеристика організаційних методів захисту інформації в комп'ютерних системах.
2. Захист інформації в комп'ютерних системах від випадкових загроз.
3. Методи і засоби захисту від електромагнітних випромінювань і наводок.
4. Захист інформації в комп'ютерних системах від несанкціонованого доступу.
5. Комп'ютерні віруси і методи боротьби з ними.
6. Захист інформації в розподілених системах.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з

дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо основні питання організаційних методів захисту інформації.

Організаційні методи захисту інформації включають заходи і дії, які повинні виконувати посадові особи в процесі створення і експлуатації комп'ютерних систем для забезпечення заданого рівня безпеки інформації.

На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в комп'ютерних системах:

- розмежування доступу до ресурсів комп'ютерної системи;
- планування заходів;
- організація робіт по розробці системи захисту інформації;
- навчання обслуговуючого персоналу і користувачів;
- сертифікація засобів захисту інформації;
- ліцензування діяльності щодо захисту інформації;
- атестація об'єктів захисту;
- удосконалення системи;
- оцінка ефективності функціонування системи захисту інформації;

– контроль виконання встановлених правил роботи в комп'ютерній системі.

За допомогою цих заходів є можливим об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації єдину комплексну систему.

1. Захист інформації в комп'ютерних системах від випадкових загроз

Для блокування випадкових загроз безпеці інформації в комп'ютерних системах доцільно вирішити комплекс завдань.

Дублювання інформації є найефективнішим способом забезпечення цілісності інформації як від випадкових загроз, так і від навмисні дій.

У залежності від цінності інформації, особливостей побудови і режимів функціонування комп'ютерної системи можуть використовуватися комп'ютерних систем можуть використовуватися такі методи дублювання.

За часом відновлювання інформації методи дублювання поділені на:

– оперативні;
– неоперативні.

До оперативних методів відносяться методи дублювання інформації, котрі дозволяють використовувати дублюючу інформацію в реальному масштабі часу. Тобто, перехід до використання дублюючої інформації здійснюється за час, який дає змогу виконати запит на використання інформації в режимі реального часу для даної комп'ютерної системи.

Усі методи, які не забезпечують виконання цих умов, відносяться до неоперативних методів дублювання.

За засобами, які використовуються для цілей дублювання, методи дублювання можна поділити на методи, що використовують:

– додаткові зовнішні запам'ятовуючі пристрої (блоки);
– зйомці носії інформації.

За числом копій методи дублювання діляться на:

– однорівневі;
– багаторівневі, але не більше трьох.

За ступенем просторової віддаленості носіїв основної і дублюючої інформації методи дублювання можуть бути:

– зосередженого дублювання;
– розосередженого дублювання.

Методами зосередженого дублювання доцільно вважати такі методи, для яких носії з основною і дубльованою інформацією знаходяться в одному приміщенні. Всі інші методи відносяться до розосередженими.

У відповідності з процедурою дублювання розрізняють методи:

– повного копіювання;
– дзеркального копіювання;
– часткового копіювання;
– комбінованого копіювання.

По виду дублювання інформації методи дублювання такі:

– методи із стиканням інформації;
– методи без стискання інформації.

У комп'ютерних системах, до яких пред'являються високі вимоги щодо збереження інформації, як правило, використовуються два резервних диски, підключених до окремих контролерів і блоків живлення.

3. Комп'ютерні віруси і методи боротьби з ними

Комп'ютерні віруси – це невеликі виконуючі програми або інтерпретовані програми, які мають властивість розповсюджуватися і самовідновлюватися в комп'ютерній системі. Віруси можуть виконувати зміну або знищення програмного забезпечення або даних ,що зберігаються в комп'ютерній системі.

Усі комп'ютерні віруси можуть бути кваліфіковані за такими ознаками:

– по середовищу знаходження;
– по способу зараження;
– по ступеню небезпеки деструктивних впливів;
– по алгоритму функціонування.

Будь-який вірус незалежно від належності до певного класу, повинен мати три функціональних блоки:

– блок зараження (розповсюдження);
– блок маскування;
– блок виконання деструктивних дій.

4. Захист інформації в розподілених комп'ютерних системах

4.1. Архітектура розподілених комп'ютерних систем:

Розподілена комп'ютерна – це множина комп'ютерних систем, зв'язаних в єдину систему за допомогою комунікаційної підсистеми.

Зосередженими комп'ютерними системами можуть бути окремі ПЄОМ, обчислювальні системи і комплекси, а також локальні обчислювальні мережі.

Розподілена комп'ютерна система у відповідності з функціональними призначенням має три підсистеми:

– користувальницька підсистема;
– підсистема управління;
– комунікаційна підсистема.

Користувальницька (абонентська) підсистема включає в себе комп'ютерні системи користувачів (абонентів) і призначена для задоволення потреб користувачів у зберіганні, обробленні і отриманні інформації.

При побудові системи захисту інформації в будь-якій розподіленій комп'ютерній системі необхідно враховувати:

– складність системи, яка визначається як кількістю підсистем, так і різноманіттям їх типів і виконуваних функцій;
– неможливість забезпечення ефективного контролю за доступом до ресурсів, розподілених на значних відстанях, можливо і за межами держави;
– можливість належності ресурсів мережі різним власникам.

1.1. *Забезпечення безпеки інформації в користувальницькій підсистемі і спеціалізованих комунікаційних комп'ютерних системах*

Особливістю захисту об'єктів розподілених комп'ютерних систем є необхідність підтримки механізмів аутентифікації і розмежування доступу віддалених процесів до ресурсів об'єкта, а також наявність в мережі спеціальних комунікаційних комп'ютерних систем. Усі елементи комунікаційної підсистеми, за винятком каналів зв'язку, розглядаються як спеціалізовані комунікаційні комп'ютерні системи.

В закритих системах робоча інформація в межах комунікаційної підсистеми циркулює в зашифрованому виді.

Розрізняють два види шифрування в комп'ютерних системах:

– шифрування в комунікаційній підсистемі – лінійне;
– межкінцеве шифрування – абонентське.

1.2. Особливості захисту інформації в базах даних

Бази даних знаходяться:

– на комп'ютерній системі користувача;
– на спеціально виділеній ЕОМ (сервері).

Захист інформації в базах даних має такі особливості:

– необхідність обліку функціонування системи управління базою даних при виборі механізмів захисту;
– розмежування доступу до інформації реалізацією не тільки на рівні файлів, але й на рівні частин баз даних.

При побудові захисту баз даних необхідно враховувати ряд специфічних загроз

безпеці інформації, пов'язаних з концентрацією в базах даних значної кількості різної інформації, а також з можливістю використання складних запитів обробки даних. Такими загрозами є:

– інференція;
– агрегірування;
– комбінація дозволених запитів для отримання закритих даних.

Протидія таким загрозам здійснюється наступними методами:

– блокування відповіді у разі невірного числа запитів;
– перекручення відповіді шляхом округлення та іншої навмисної корекції даних;
– розділ баз даних;
– випадковий вибір запису для обробки;
– контекстно-орієтированний захист;
– контроль запитів, що поступають.

II. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 9. Загальні методи забезпечення інформаційної безпеки
Практичне заняття: Загальні методи забезпечення інформаційної безпеки
Навчальна мета заняття: розглянути основні методи і засоби захисту інформації у загальнодержавних і телекомунікаційних системах.
Кількість годин: 2 год.
Навчальні питання:

1. Правові методи забезпечення інформаційної безпеки.
2. Організаційно-технічні методи забезпечення інформаційної безпеки.
3. Економічні методи забезпечення інформаційної безпеки.
4. Забезпечення інформаційної безпеки у загальнодержавних і телекомунікаційних системах.
5. Забезпечення інформаційної безпеки у правоохоронній та судових сферах.

Література:
Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та

ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо правові методи забезпечення інформаційної безпеки.

До *правових методів забезпечення інформаційної безпеки* України належать розробка нормативних правових актів, що регламентують відносини у інформаційній сфері, і нормативних методичних документів із питань забезпечення інформаційної безпеки України. Найважливішими напрямами цієї діяльності є:

– внесення змін і доповнень до законодавства України, що регулює відносини в галузі забезпечення інформаційної безпеки, з метою створення й удосконалення системи забезпечення інформаційної безпеки України;

– законодавче розмежування повноважень у галузі забезпечення інформаційної безпеки України між органами державної влади,визначення цілей, завдань і механізмів участі в цій діяльності громадських об'єднань, організацій і громадян;

– розробка та прийняття нормативних правових актів України, які установлюють відповідальність юридичних і фізичних осіб за несанкціонований доступ до інформації;

– уточнення статусу іноземних інформаційних агентств, засобів масової інформації та журналістів, а також інвесторів при залученні іноземних інвестицій для розвитку інформаційної інфраструктури України;

– законодавче закріплення пріоритету розвитку національних мереж зв'язку і вітчизняного виробництва космічних супутників зв'язку;

– визначення статусу організацій, що надають послуги глобальних інформаційно-телекомунікаційних мереж на території України, і правове регулювання діяльності цих організацій.

2. Організаційно-технічні методи забезпечення інформаційної безпеки

Організаційно-технічними методами забезпечення інформаційної безпеки України є:

– створення й удосконалення системи забезпечення інформаційної безпеки України;

– розробка, використання й удосконалення засобів захисту інформації і методів контролю ефективності цих засобів, розвиток захищених телекомунікаційних систем, підвищення надійності спеціального програмного забезпечення;

– створення систем і засобів запобігання несанкціонованому доступу до інформації, що обробляється, і спеціальним впливам, які призводять до руйнування, знищення, спотворення інформації, а також зміна штатних режимів функціонування систем і засобів та зв'язку;

– виявлення технічних пристроїв і програм, що загрожують нормальному функціонуванню інформаційно-телекомунікаційних систем, запобігання перехопленню інформації у технічних каналах її витоку, застосування криптографічних засобів захисту інформації під час її обробки та передачі каналами зв'язку, контроль за виконанням спеціальних вимог із захисту інформації;

– сертифікація засобів захисту інформації, ліцензування діяльності в галузі захисту інформації, стандартизація способів і засобів її захисту;

– контроль за діями персоналу в захищених інформаційних системах, підготовка кадрів у галузі забезпечення інформаційної безпеки України;

– формування системи моніторингу показників і характеристик інформаційної безпеки України у найважливіших сферах життя і діяльності суспільства та держави.

3. Економічні методи забезпечення інформаційної безпеки

Економічні методи забезпечення інформаційної безпеки України містять:

– розробку програм забезпечення інформаційної безпеки України та визначення порядку їх фінансування;

– удосконалення системи фінансування робіт з реалізації правових і організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних і юридичних осіб.

4. Забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах

Основними напрямами забезпечення інформаційної безпеки України *в загальнодержавних інформаційних і телекомунікаційних системах* є:

– запобігання перехопленню за допомогою технічних засобів розвідки інформації з приміщень і з об'єктів, а також інформації, яка передається каналами зв'язку;

– запобігання несанкціонованого доступу до інформації, яка оброблюється чи зберігається в технічних засобах інформатизації;

– запобігання витоку інформації технічними каналами під час експлуатації технічних засобів її обробки, зберігання та передавання;

– запобігання здійсненню спеціальних програмно-технічних впливів, які призводять до руйнування, знищення, спотворення інформації чи збоїв у роботі засобів інформатизації;

– забезпечення інформаційної безпеки при підключенні загальнодержавних інформаційних і телекомунікаційних систем до зовнішніх інформаційних мереж, включаючи міжнародні;

– забезпечення безпеки інформації обмеженого доступу при взаємодії інформаційних і телекомунікаційних систем різних класів захищеності;

– виявлення впроваджених на об'єкти інформатизації та в технічні засоби електронних пристроїв перехоплення інформації.

5. Забезпечення інформаційної безпеки України у правоохоронній і судовій сферах

До найважливіших об'єктів забезпечення інформаційної безпеки у правоохоронній і судовій сферах належать:

– інформаційні ресурси органів державної виконавчої влади, які реалізують правоохоронні функції, судових органів, їх інформаційно-обчислювальних центрів, науково-дослідних установ і навчальних закладів, що містять спеціальні відомості та оперативні дані службового характеру;

– інформаційно-обчислювальні центри, їх інформаційне, технічне, програмне та нормативне забезпечення;

– інформаційна інфраструктура (інформаційно-обчислювальні мережі, пункти керування, вузли та лінії зв'язку).

Поряд *із загальними методами та засобами захисту інформації застосовуються також специфічні методи і засоби забезпечення інформаційної безпеки у правоохоронній і судовій сферах*. Головними з них є:

– створення захищеної багаторівневої системи інтегрованих банків даних оперативно-розшукового, довідкового, криміналістичного і статистичного характеру на базі спеціалізованих інформаційно-телекомунікаційних систем;

– підвищення рівня професійної та спеціальної підготовки користувачів інформаційних систем.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 10. Засадничі принципи боротьби з кіберзлочинністю
Практичне заняття: Побудова комплексних систем захисту інформації.

Навчальна мета заняття: розглянути основні методи і засоби захисту інформації у загальнодержавних і телекомунікаційних системах.

Кількість годин: 2 год.

Навчальні питання:

1. Концепція організації захищених комп'ютерних систем.
2. Етапи створення комплексної системи захисту комп'ютерних систем.
3. Науково-дослідницька розробка комплексної системи захисту інформації.
4. Вибір показників ефективності та критеріїв оптимальності комплексної системи захисту інформації.
5. Створення організаційної структури комплексної системи захисту інформації.
6. Організація функціонування комплексних систем захисту інформації.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. - 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо концепцію організації захищених комплексних систем захисту інформації

Системи захисту інформації відносяться до класу складних систем і для їх побудови можуть використовуватися основні принципи побудови складних систем із врахуванням специфіки завдань, що вирішуються:

– паралельна розробка комп'ютерної системи і системи захисту інформації;
– системний підхід до побудови захищеної комп'ютерної системи;
– багаторівнева структура системи захисту інформації;
– блочна архітектура захищеної комп'ютерної системи;
– можливість розвитку системи захисту інформації;
– дружній інтерфейс захищеної комп'ютерної системи з користувачами і обслуговуючим персоналом.

Система захисту інформації повинна мати декілька рівнів, що перекривають один одного, тобто, щоб добратися до закритої інформації, зловмиснику необхідно «зруйнувати» всі рівні захисту. Наприклад, для окремого об'єкта комп'ютерної системи можна виділити 6 рівнів захисту:

– охорона по периметру території об'єкта;
– охорона по периметру будівлі;
– охорона приміщення;
– захист апаратних засобів;
– захист програмних засобів;
– захист інформації.

Комплексна система захисту інформації повинна бути дружньою по відношенню до користувачів і обслуговуючого персоналу, а саме:

– повинна бути максимально автоматизованою і не вимагати від користувача виконання значного об'єму дій, пов'язаних з системою захисту інформації;
– не створювати обмежень у виконанні користувачем своїх службових обов'язків;

– доцільним є передбачення заходів щодо зняття інформації з пристроїв, які відмовили для відновлення їх робото здатності.

–

1. Етапи створення комплексної системи захисту інформації

У залежності від особливостей комп'ютерної системи, умови її експлуатації і вимог до захисту інформації процес створення комплексної системи захисту може не вміщувати окремих етапів, або зміст їх може частково відрізнятися від загальноприйнятих норм при розробці складних апаратно-програмних систем. Розробка таких систем включає наступні етапи:

– розробка технічного завдання (науково-дослідна розробка);
– ескізне проектування;
– технічне проектування;
– робоче проектування;
– виробництво дослідного зразка.

Одним із основних етапів розробки комплексної системи захисту інформації є етап розробки технічного завдання.

2. Науково-дослідна розробка комплексної системи захисту інформації

Науково-дослідна розробка починається з аналізу загроз безпеці інформації, аналізу комп'ютерної системи, що захищається і аналізу конфіденційності та важливості інформації, яка повинна оброблятися, зберігатися і передаватися в комп'ютерній системі. На основі аналізу робиться висновок щодо доцільності створення комплексної системи захисту інформації. На основі аналізу інформації визначаються вимоги до її захищеності.

Так як комплексна система захисту інформації є підсистемою комп'ютерної системи, то взаємодія системи захисту з комп'ютерною системою можна визначити як внутрішню, а взаємодію із зовнішнім середовищем – як зовнішню.

Внутрішні умови взаємодії визначаються архітектурою комп'ютерної системи. При цьому враховуються:

– географічне положення комп'ютерної системи;
– тип комп'ютерної системи (розподілений або зосереджений);
– структура комплексної системи (технічна, програмна, інформаційна тощо);
– надійність и продуктивність;
– типи апаратних і програмних засобі, які використовуються, і режими їх роботи;
– загрози безпеці інформації, які виникають всередині комп'ютерної системи (відмови апаратних і програмних засобів, алгоритмічні помилки тощо).

Враховуються наступні зовнішні умови:

– взаємодія із зовнішніми умовами;
– випадкові і навмисні загрози.

Модель загроз розглядається і як композиція моделі загроз злочинця і моделі випадкових загроз. Моделі надаються у вигляді таблиць, графів або на вербальному рівні. При побудові моделі зловмисника використовуються два підходи:

– модель орієнтується тільки на висококваліфікованого зловмисника-професіонала, який має легальний доступ на всіх рубежах захисту;

– модель враховує кваліфікацію зловмисника, його можливості та офіціальний статус в комп'ютерній системі.

Перший підхід легше реалізується і дозволяє визначити верхню межу преднамеренніх загроз безпеці інформації.

Другий підхід відрізняється гнучкістю і дає змогу враховувати особливості комп'ютерної системи в повній мірі. Градація зловмисників за їх кваліфікацією ділиться на три класи:

– висококваліфікований зловмисник-професіонал;
– кваліфікований зловмисник-професіонал;
– некваліфікований зловмисник-непрофесіонал.

4. Вибір показників ефективності та критеріїв оптимальності комплексної системи захисту інформації

Ефективність систем оцінюється за допомогою показників ефективності.

Показник ефективності характеризує ступінь відповідності оцінюваної системи своєму призначенню.

Використовуються кількісні та якісні характеристики.

Кількісні характеристики систем мають числове значення (їх називають також параметрами).

Якісні характеристики визначають наявність (відсутність) певних режимів, захисних механізмів або порівняльний ступінь властивостей систем (добре, задовільно, краще, гірше).

Щоб оцінити ефективність системи захисту інформації або порівняти системи за їх ефективністю, необхідно задати деяке правило переваг. Для отримання критеріїв ефективності при використанні деякої множини k показників використовують ряд підходів.

1. Вибираємо один головний показник, і оптимальною називається система, для якої цей показник досягає максимуму, за умови, що інші показники задовольняють систему обмежень, заданих у виді нерівностей.

2. Методи, засновані на ранжуванні показників за важливістю. При порівнянні систем однойменні показники ефективності співпадають в порядку зменшення їх важливості за визначеними алгоритмами. Прикладами таких методів можуть бути лексикографічний метод і метод послідовних поступок.

3. Мультиплікативні і адитивні методи отримання критеріїв ефективності ґрунтуються на об'єднанні усіх або частини показників за допомогою операцій множення або складання в узагальненні показники.

4. Система захисту інформації може здійснюватися методом Парето, сутність якого полягає в тому, що при використанні n показників ефективності системі відповідає точка n-мірному просторі. В n-мірному просторі будується область парето-оптимальних рішень, в якій для непорівняльних показників покращення будь-якого параметру неможливо без погіршення інших показників ефективності.

5. Створення організаційної структури комплексної системи захисту інформації

Організаційна система захисту інформації призначена для виконання організаційних способів захисту, експлуатації технічних, програмних і криптографічних засобів захисту, а також контролю за виконанням встановлених правил експлуатації комп'ютерної системи обслуговуючим персоналом і користувачами. Такі структури входять до складу служб безпеки відомств, корпорацій, організацій.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Тема № 11. Методи боротьби з кіберзлочинністю за межами України

Практичне заняття № 11. Загальні методи забезпечення інформаційної безпеки за межами України

Навчальна мета заняття: розглянути основні методи і засоби захисту інформації за межами України.

Кількість годин: 2 год.

Навчальні питання:

1. Правові методи боротьби з кіберзлочинністю та забезпечення інформаційної безпеки за межами України..

2. Економічні методи забезпечення інформаційної безпеки за межами України.

Література:

Основна

1. Програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
2. Робоча програма навчальної дисципліни «Вступ у спеціальність». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2020 р.
3. Тулупов В.В. Вступ у спеціальність. Електронний курс лекцій. Харків, ХНУВС, 2020 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних занять з дисципліни " Вступ у спеціальність ". Харків, ХНУВС, 2020 р.
5. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
6. Юдін О.К., Богуш В.М. Інформаційна безпека держави. — Харків: Консум, 2012. — 576 с.
7. Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.
8. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
9. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

Додаткова

10. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і безпека. – 2014. –№ 2 (53). – С. 38-42
11. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
12. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
13. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «Поліграф Консалтинг», 2003. 286 с.
14. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
15. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Нормативно-правові акти

16. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
17. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
18. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
20. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
21. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
23. Robertson N. Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe [Електронний ресурс] / N. Robertson, P. Cruickshank, T. Lister. – Режим доступу : http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1.
24. Shelley L. Organized Crime, Terrorism and Cybercrime [Електронний ресурс] / L. Shelley; перевод исследователя ВЦИОП Тропиной Т.Л. – Режим доступу : http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття:

І. Порядок проведення вступу до заняття.

Розглянемо правові методи забезпечення інформаційної безпеки за межами України.

До *правових методів забезпечення інформаційної безпеки* України належать розробка нормативних правових актів, що регламентують відносини у інформаційній сфері, і нормативних методичних документів із питань забезпечення інформаційної безпеки України. Найважливішими напрямами цієї діяльності є:

– внесення змін і доповнень до законодавства України, що регулює відносини в галузі забезпечення інформаційної безпеки, з метою створення й удосконалення системи забезпечення інформаційної безпеки України;

– законодавче розмежування повноважень у галузі забезпечення інформаційної безпеки України між органами державної влади,визначення цілей, завдань і механізмів участі в цій діяльності громадських об'єднань, організацій і громадян;

– розробка та прийняття нормативних правових актів України, які установлюють відповідальність юридичних і фізичних осіб за несанкціонований доступ до інформації;

– уточнення статусу іноземних інформаційних агентств, засобів масової інформації та журналістів, а також інвесторів при залученні іноземних інвестицій для розвитку інформаційної інфраструктури України;

– законодавче закріплення пріоритету розвитку національних мереж зв'язку і вітчизняного виробництва космічних супутників зв'язку;

– визначення статусу організацій, що надають послуги глобальних інформаційно-телекомунікаційних мереж на території України, і правове регулювання діяльності цих організацій.

2. Організаційно-технічні методи забезпечення інформаційної безпеки

Організаційно-технічними методами забезпечення інформаційної безпеки України є:

– створення й удосконалення системи забезпечення інформаційної безпеки України;

– розробка, використання й удосконалення засобів захисту інформації і методів контролю ефективності цих засобів, розвиток захищених телекомунікаційних систем, підвищення надійності спеціального програмного забезпечення;

– створення систем і засобів запобігання несанкціонованому доступу до інформації, що обробляється, і спеціальним впливам, які призводять до руйнування, знищення, спотворення інформації, а також зміна штатних режимів функціонування систем і засобів та зв'язку;

– виявлення технічних пристроїв і програм, що загрожують нормальному функціонуванню інформаційно-телекомунікаційних систем, запобігання перехопленню інформації у технічних каналах її витоку, застосування криптографічних засобів захисту інформації під час її обробки та передачі каналами зв'язку, контроль за виконанням спеціальних вимог із захисту інформації;

– сертифікація засобів захисту інформації, ліцензування діяльності в галузі захисту інформації, стандартизація способів і засобів її захисту;

– контроль за діями персоналу в захищених інформаційних системах, підготовка кадрів у галузі забезпечення інформаційної безпеки України;

– формування системи моніторингу показників і характеристик інформаційної безпеки України у найважливіших сферах життя і діяльності суспільства та держави.

3. Економічні методи забезпечення інформаційної безпеки

Економічні методи забезпечення інформаційної безпеки України містять:

– розробку програм забезпечення інформаційної безпеки України та визначення порядку їх фінансування;

– удосконалення системи фінансування робіт з реалізації правових і організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних і юридичних осіб.

4. Забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах

Основними напрямами забезпечення інформаційної безпеки України *в загальнодержавних інформаційних і телекомунікаційних системах* є:

– запобігання перехопленню за допомогою технічних засобів розвідки інформації з приміщень і з об'єктів, а також інформації, яка передається каналами зв'язку;

– запобігання несанкціонованого доступу до інформації, яка оброблюється чи зберігається в технічних засобах інформатизації;

– запобігання витоку інформації технічними каналами під час експлуатації технічних засобів її обробки, зберігання та передавання;

– запобігання здійсненню спеціальних програмно-технічних впливів, які призводять до руйнування, знищення, спотворення інформації чи збоїв у роботі засобів інформатизації;

– забезпечення інформаційної безпеки при підключенні загальнодержавних інформаційних і телекомунікаційних систем до зовнішніх інформаційних мереж, включаючи міжнародні;

– забезпечення безпеки інформації обмеженого доступу при взаємодії інформаційних і телекомунікаційних систем різних класів захищеності;

– виявлення впроваджених на об'єкти інформатизації та в технічні засоби електронних пристроїв перехоплення інформації.

5. Забезпечення інформаційної безпеки України у правоохоронній і судовій сферах

До найважливіших об'єктів забезпечення інформаційної безпеки у правоохоронній і судовій сферах належать:

– інформаційні ресурси органів державної виконавчої влади, які реалізують правоохоронні функції, судових органів, їх інформаційно-обчислювальних центрів, науково-дослідних установ і навчальних закладів, що містять спеціальні відомості та оперативні дані службового характеру;

– інформаційно-обчислювальні центри, їх інформаційне, технічне, програмне та нормативне забезпечення;

– інформаційна інфраструктура (інформаційно-обчислювальні мережі, пункти керування, вузли та лінії зв’язку).

Поряд *із загальними методами та засобами захисту інформації застосовуються також специфічні методи і засоби забезпечення інформаційної безпеки у правоохоронній і судовій сферах*. Головними з них є:

– створення захищеної багаторівневої системи інтегрованих банків даних оперативно-розшукового, довідкового, криміналістичного і статистичного характеру на базі спеціалізованих інформаційно-телекомунікаційних систем;

– підвищення рівня професійної та спеціальної підготовки користувачів інформаційних систем.

ІІ. Порядок проведення основної частини заняття. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань. Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття. Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.