Відокремлений підрозділ
«МИКОЛАЇВСЬКИЙ ФАКУЛЬТЕТ МЕНЕДЖМЕНТУ І БІЗНЕСУ КИЇВСЬКОГО УНІВЕРСИТЕТУ КУЛЬТУРИ»

Кафедра загально-професійних та соціально-гуманітарних дисциплін

ЗАХИСТ ІНФОРМАЦІЇ

Методичні рекомендації до самостійної роботи студентів спеціальності 029 «Інформаційна, бібліотечна та архівна справа»

МИКОЛАЇВ – 2021

Захист інформації : методичні рекомендації для самостійної роботи студентів спеціальності 029 «Інформаційна, бібліотечна та архівна справа». – Миколаїв: ВП «МФ КНУКіМ», 2021. 14 с.

Розробник: Сидоренко А. І., кандидат педагогічних наук, доцент.

Наведено завдання з самостійної роботи та список рекомендованої літератури для студентів спеціальності «Інформаційна, бібліотечна та архівна справа».

Рецензенти:

Кандидат наук із соц. комунікацій, директор наукової бібліотеки Національного університету кораблебудування імені адмірала Макарова Костирко Т. М.

Розглянуто і схвалено рішенням кафедри загально-професійних та соціально-гуманітарних дисциплін ВП «Миколаївський факультет менеджменту і бізнесу Київського університету культури»

Протокол № 1 від 31 серпня 2021 р.

Мета навчальної дисципліни «Захист інформації» – надання студентам знань, пов'язаних з інформаційною діяльністю суспільства як сферою правового захисту, а також вивчення організаційного і технічного аспектів його забезпечення.

Завдання навчальної дисципліни:

- розкрити об'єкт, предмет, структуру, міждисциплінарні зв'язки дисципліни «Захист інформації»;
- ознайомити студентів з понятійним апаратом дисципліни;
- виробити вміння розмежовувати сферу конфіденційної інформації та інформації загального користування;
- забезпечити засвоєння своїх не лише загальногромадянських, а й фахових прав і обов'язків в аспекті володіння і користування інформацією як власністю суспільства, того чи іншого державного або управлінського органу, фірми, підприємства;
- освоїти відповідні технології, обумовлені потребою захисту інформації.

Предметом вивчення навчальної дисципліни є інформація, її властивості, процеси, методи й засоби її обробки (збір, пошук, введення, зберігання, перетворення, видача за заданими критеріями), а також принципи побудови і технології роботи з системами захисту даних та інструментальні засоби для підтримки інформаційної безпеки.

студент повинен знати:

- понятійно-термінологічну базу курсу;
- основні поняття інформаційного права, нормативно-правової бази захисту інформації в Україні та за її межами;
- причини виникнення збоїв в АС та локальних мережах, планування дій щодо їх попередження;
- основні загрози безпеці інформації АС;
- шляхи витоку інформації;
- способи та методів забезпечення захисту інформації в АС, склад необхідної документації для його забезпечення;
- шляхи зараження АС комп'ютерними вірусами, ознаки їх прояви, програм й основних заходів щодо виявлення й захисту від вірусів;
- захисні механізми ОС MS Windows; способи резервування інформації;
- правила поведінки користувача в аварійних ситуаціях, підходів щодо відновлення роботи АС та мереж;
- вимоги до охорони праці користувачів ПК, організації безпечного ергономічного робочого місця спеціаліста з точки зору безпеки інформаційного документу, дотримання норм ПТБ та ПБ.

уміти:

- оперувати нормативно-правовими актами із захисту інформації;
- формувати власну концепцію побудови системи захисту інформації;

- створювати та аналізувати захисні бар'єри в захисті інформації, яка циркулює в локальних і глобальних мережах, Internet;
- використовувати інформаційні технології при виконанні фахових завдань, пов'язаних із захистом інформації;
- виконати аналіз середовищ, з яких складається АС та шляхів витоку інформації;
- виконати вхід до комп'ютера з підключенням до локальної мережі та в автономному режимі;
- виконати апаратне та програмне підключення/відключення периферійних пристроїв через порти комп'ютера та резервування інформації через них;
- володіти основними прийомами створення нових облікових записів користувачів ОС MS Windows, надання їм необхідних прав доступу, встановлення та зміни паролів;
- шифрувати інформаційний документ під файловою системою NTFS;
- завантажувати необхідне програмне забезпечення (прикладне та сервісне);
- виконувати архівацію файлів (папок) з встановленням паролів на створені архіви;

мати навички:
- складання переліку необхідної документації для захисту АС та інформаційного документу;
- складання моделі порушника;
- виконувати архівацію файлів (папок) з встановленням паролів на створені архіви;
- розпізнавання зараження комп'ютерів вірусами за відомими ознаками;
- виконувати архівацію файлів (папок) з встановленням паролів на створені архіви.
- організації безпечного автоматизованого робочого місця фахівця з точки зору захисту інформації, ергономіки та охорони праці.

Міждисциплінарні зв'язки: вивчення курсу інтегрується на системі професійних знань з дисциплін «Документознавство», «Комп'ютерні технології, системи і мережі», «Інтернет-ресурси», «Офісні технології в документаційній діяльності» тощо.

ТЕМИ І ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Тема 1.1. Вступна лекція

Теоретичні питання

1. Що вивчає дисципліна «Захист інформації?».
2. Який зв'язок між курсами «Захист інформації» та «Комп'ютерні технології, системи і мережі»?
3. Сформулюйте мету навчальної дисципліни «Захист інформації»?
4. У чому полягають завдання курсу «Захист інформації»?

5. Яка роль захисту інформації у практичній роботі фахівця інформаційної сфери?

Практичні завдання

Скласти рекомендований перелік праць сучасних дослідників до навчальної дисципліни «Захист інформації».

Література: 4,6,16,35,38,45,47,49

Тема 1.2 Основні поняття інформаційного права та захисту інформації

Теоретичні питання

1. Що таке інформаційна безпека; інформаційна безпека держави, нації (національна інформаційна безпека), суспільства, міжнародна регіональна та глобальна інформаційна безпека?
2. В чому полягає особливість інформаційної безпеки соціальної спільноти (організації), у тому числі: інформаційна безпека підприємництва, комерційної та інших видів господарської діяльності?

Практичні завдання

1. Дайте перелік основних законодавчих та нормативних документів з питань захисту інформації.
2. Проаналізувати історію розвитку (онтологія) інформаційних технічних засобів (та технологій) соціальних комунікації.
3. Охарактеризувати соціологічний, соціально-економічнпй, соціально-психологічний, моральний, правовий аспекти інформаційної безпеки.
4. Розкрити зміст категорії «інформаційна безпека» в залежності від рівня її об'єктивізації та суб'єктивної приналежності.
5. Зробити порівняльний аналіз змістової наповненості категорій «інформаційна безпека» та «захист інформації».
6. Визначити проблеми правового регулювання захисту інформації в АС.

Література: 1,2,7,11,21-24,34,46-47,55-57,60,76

Тема 1.3. Комплексна система захисту інформації

Теоретичні питання

1. Дайте визначення поняття «комплексна система захисту інформації».
2. Які особливості витоку інформації, що поширюються акустичними каналами?
3. Назвіть складові комплексної системи захисту інформації.

Практичні завдання

1. Опрацювати тему за лекційним матеріалом і списком рекомендованої літератури, підготуватися до опитування за питаннями для самоперевірки.
2. Назвіть основні завдання служби захисту інформації.
3. Охарактеризуйте інженерно-технічні заходи забезпечення інформаційної безпеки.

4. Назвіть методи адміністративного впливу в забезпеченні захисту інформації.
5. Охарактеризувати використання організаційних каналів витоку інформації для промислового шпигунства.

Література: 8,15-18,25,31,34,37,48-49,51-53,65,67,68,79-80.

ТЕМА 1.4. Способи і методи забезпечення безпеки інформації в комп'ютерних системах і мережах

Теоретичні питання

1. Якими є місце і роль дисциплінарних заходів щодо захисту інформації?
2. Яка роль патентного та ліцензійного права щодо захисту інформації: забезпечення інформаційної безпеки?
3. Яка роль трудового права у регулюванні відносин щодо захисту інформації?
4. Яким чином співвідносяться інтереси роботодавців і працівників щодо захисту інформації?

Практичні завдання

1. Опрацювати тему за лекційним матеріалом і списком рекомендованої літератури, підготуватися до опитування за питаннями для самоперевірки.
2. Назвіть захисні механізми операційних систем.

Література: 8,15-18,25,31,34,37,48-49,51-53,65,67,68

Тема 1.5.Основні юридичні делікти з інформаційної безпеки в соціально-інформаційних відносинах

Теоретичні питання

1. Охарактеризуйте інформацію як предмет злочинного посягання та як засіб вчинення злочинів.
2. Яка класифікація юридичних деліктів у сфері інформаційних правовідносин?
3. Яка класифікація суб'єктів юридичних деліктів?

Практичні завдання

1. Опрацювати тему за лекційним матеріалом і списком рекомендованої літератури, підготуватися до опитування за питаннями для самоперевірки.
2. Підготувати відповіді на наступні питання:

- Поняття юридичного делікту в інформаційних правовідносинах.
- Класифікація юридичних деліктів в сфері інформаційних правовідносин.
- Класифікація суб'єктів юридичних деліктів в сфері інформаційних відносин.
- Дайте визначення поняттям «хакер», «крекер».

Література: 8,15-18,25,31,34,37,48-49,51-53,65,67,68

Тема 1.6. Організація роботи з персоналом з питань інформаційної безпеки

Теоретичні питання

1. Які особливості співбесіди при доборі персоналу для роботи з конфіденційною інформацією?
2. Які особливості звільнення персоналу, який працював з інформацією з обмеженим доступом?
3. Розкрийте сутність і зміст навчання персоналу, який працюватиме з інформацією з обмеженим доступом.

Практичні завдання

1. Дати письмові відповіді на наступні питання:
   - Охарактеризувати технологію прийому співробітників, робота яких пов'язана з конфіденційною інформацією.
   - Розкрити особливості трудового договору з працівником, робота якого пов'язана з конфіденційною інформацією.
   - Дати перелік принципів побудови дозвільної системи доступу та розкрити її значення.
   - Визначити завдання поточної роботи з персоналом, який володіє конфіденційною інформацією.
   - Дати аналіз основних форм контролю якості роботи персоналу, який володіє конфіденційною інформацією.

Література: 8,15-18,25,31,34,37,48-49,51-53,65,67,68,79-80

РОЗДІЛ 2. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ СЕРЕДОВИЩІ

Тема 2.1. Комп'ютерні віруси та антивірусні програми

Теоретичні питання

1. Назвіть види комп'ютерних вірусів.
2. Поняття вірусу.
3. Яким чином проявляється дія вірусу на файли?
4. Які існують джерела вірусів?
5. Яких рекомендацій потрібно дотримуватися для уникнення вірусів?
6. Які програми використовують для боротьби з вірусами?
7. Основні групи вірусів.
8. Методи захисту від комп'ютерних вірусів.
9. Антивірусна програма АУК
10. Антивірусна програма «Український Національний антивірус».
11. Поновлення антивірусних баз.
12. Дії користувача при зараженні комп'ютеру вірусами.
13. Які сучасні антивірусні програми Ви знаєте?
14. Які сучасні антивірусні програми Ви використовуєте?

Практичні завдання

1. Опрацювати тему за лекційним матеріалом і списком рекомендованої літератури, підготуватися до опитування за питаннями для самоперевірки.
2. Охарактеризуйте антивірусну програму Касперського. Які її переваги і недоліки?
3. Підготуйте презентацію на тему: «Методи захисту від комп'ютерних вірусів».
4. Охарактеризуйте сучасні антивірусні програми.

Література: 8,15-18,25,31,34,37,53

Тема 2.2. Криптографічний захист інформації

Теоретичні питання

1. Дайте визначення поняттям: «криптографія», криптоаналіз».
2. Що таке шифрувальна технологія?
3. Які види криптосистем Ви знаєте?
4. Способи криптографічного захисту інформації.

Практичні завдання

1. Охарактеризуйте один вітчизняний та один зарубіжний стандарти шифрування даних.
2. Створення презентації за даною темою (15-20 слайдів).
3. Обговорення питань:
   - Поняття та суть криптографічного захисту інформації.
   - Методи симетричної та асиметричної криптографії.
   - Криптографічні протоколи.
   - Стандарт шифрування даних.
   - Головні застережні заходи при роботі з паролями.
   - Цифровий підпис.

Література: 5,9,13,20,70

Тема 2.3. Особливості захисту інформації в мережі Інтернет

Теоретичні питання

1. Які існують типи комп'ютерних мереж?
2. Який принцип адресації існує в мережах?
3. Які принципи організації мережі Інтернет?
4. Які основні сервісні можливості мережі Інтернет?
5. Що означають домени верхнього рівня?
6. Які логічні оператори використовуються при введенні пошукового виразу в інформаційно-пошукову систему?
7. Чи всі пошукові системи мають однаковий синтаксис пошукової мови?
8. Поняття провайдерства.
9. Апаратні засоби для Інтернет. Модеми. Швидкість передачі даних.
10. Основні технології підключення до Інтернет.

11. Програма Internet Explorer.
12. Структура Веб-адреси.
13. Інформаційно-пошукові системи Росії та України.
14. Використання гіперпосилань.
15. Збереження знайденого матеріалу у власних файлах.

Практичні завдання

1. Опрацювати тему за лекційним матеріалом і списком рекомендованої літератури, підготуватися до опитування за питаннями для самоперевірки.
2. Визначити особливості захисту інформації в глобальній мережі Інтернет.
3. Вивчити параметри роботи програми MS Internet Explorer.
4. Навчитися знаходити в Інтернет та зберігати на жорсткому диску Вашого комп'ютера необхідні веб-сторінки.
5. Здійснити аналіз діяльності українських та російських фірм, що працюють у сфері інформаційних технологій.

Література: 4,8,15,25,28,30,32-33,37,44,45,49-52,54,61-64,66,69

Тема 2.4. Організація безпечного ергономічного робочого місця фахівця з точки зору безпеки інформаційного документу, дотримання норм ПТБ та ПБ

Теоретичні питання

1. Які існують стандарти з охорони праці на ПК?
2. Назвіть оптимальні й припустимі параметри температури й відносної вологості повітря в приміщеннях із ПК?

Практичні завдання

1. Підготувати методичні рекомендації працівникам на тему: «Охорона праці користувачів ПК».
2. Створити презентацію на тему: «Обов’язки, права та відповідальність за порушення правил безпечної обробки інформації та інформаційного документу».

Література: 38,39,40,56

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Законодавчо-нормативні видання України[1]

1. Конституція України (ст. 17).
2. Кримінальний кодекс України, прийнятий постановою ВР України від

[1] Тексти законодавчо-нормативних видань України отримані з Української Мережі ділової інформації "ЛІГАБізнесІнформ" (веб-сайт http://www.liga.net), офіційних веб-сайтів Верховної Ради України (,http://www.rada.gov.ua), Президента України (http://www.president.gov.ua) та Кабінету Міністрів України *(*http://www. *kmu.gov. ua).*

2001.04.05 №2341-111 (опубл. "Відомості Верховної Ради України", 2001 р., №№ 25 - 26, ст. 163, 176, 216, 301, 361-363).

3. Закон України від 2006.02.23 № 3475-IV "Про Державну службу спеціального зв'язку та захисту інформації України"

4. Закон України від 2003.11.18 № 1280-IV "Про телекомунікації"

5. Закон України від 2003.05.22 № 852-IV "Про електронний цифровий підпис"

6. Закон України від 2002.01.10 № 2919-III "Про Національну систему конфіденційного зв'язку"

7. Закон України від 2001.09.13 № 2680-III "Про внесення змін до деяких законів України за результатами парламентських слухань "Проблеми інформаційної діяльності, свободи слова, дотримання законності та стан інформаційної безпеки України"

8. Закон України від 1994.07.05 № 80/94 "Про захист інформації в інформаційно-телекомунікаційних системах"

9. Закон України від 1994.01.21 № 3855-XII "Про державну таємницю"

10. Закон України від 1992.10.02 № 2657-XII "Про інформацію"

11. Концепція (Основи державної політики) національної безпеки України. Схвалено постановою Верховної Ради України від 1997.01.16 №3/97-ВР

12. Указ Президента України від 2002.09.18 № 836/2002 "Про заходи щодо забезпечення інформаційної безпеки держави"

13. Указ Президента України від 2002.07.04 № 614/2002 "Питання забезпечення діяльності Національної системи конфіденційного зв'язку"

14. Указ Президента України від 2002.01.22 № 63/2002 "Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України"

15. Указ Президента України від 2001.09.24 № 891/2001 "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних"

16. Указ Президента України від 2000.10.06 № 1120/2000 "Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України"

17. Указ Президента України від 2000.04.10 № 582/2000 "Про заходи щодо захисту інформаційних ресурсів держави"

18. Указ Президента України від 1999.09.27 № 1229/99 "Про Положення про технічний захист інформації в Україні"

19. Указ Президента України від 1998.05.22 № 505/98 "Про Положення про порядок здійснення криптографічного захисту інформації в Україні"

20. Указ Президента України від 1998.02.11 № 110/98 "Про заходи щодо вдосконалення криптографічного захисту інформації в телекомунікаційних та

інформаційних системах"

21. Постанова Верховної Ради України від 2006.02.21 № 3454-IУ "Про прийняття за основу проекту Закону України про затвердження Національної стратегії розвитку інформаційного суспільства в Україні на 2006 - 2015 роки"

22. Постанова Верховної Ради України від 2003.04.03 № 687-IУ "Про Концепцію національної інформаційної політики"

23. Постанова Верховної Ради України від 2001.06.07 № 2498-III "Про підсумки парламентських слухань "Проблеми інформаційної діяльності, свободи слова, дотримання законності та стану інформаційної безпеки України""

24. Постанова Верховної Ради України від 1999.09.21 № 1072-XIУ "Про проект Закону України про інформаційний суверенітет та інформаційну безпеку України"

25. Постанова КМ України від 29 березня 2006 р. № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"

26. Постанова КМ України від 2004.10.28 № 1452 "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності"

27. Постанова КМ України від 2004.07.13 № 903 "Про затвердження Порядку акредитації центру сертифікації ключів"

28. Постанова КМ України від 2002.11.16 № 1772 "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах"

29. Постанова КМ України від 2002.10.11 № 1520 "Про затвердження Державної програми створення, розвитку та забезпечення функціонування Національної системи конфіденційного зв'язку"

30. Постанова КМ України від 2002.04.12 № 522 "Про затвердження Порядку підключення до глобальних мереж передачі даних"

31. Постанова КМ України від 2002.03.13 № 281 "Про деякі питання захисту інформації, охорона якої забезпечується державою"

32. Постанова Кабінету Міністрів України від 2006.03.13 №373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних[y] та інформаційно-телекомунікаційних системах"

33. Постанова КМ України від 2001.05.06 № 483 "Про утворення Інституту телекомунікацій та глобального інформаційного простору Національної академії наук"

34. Постанова КМ України, від 1997.10.08 № 1126 "Про затвердження Концепції технічного захисту інформації в Україні"

35. Наказ|Положення Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 2002.02.23 № 9 "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб"

36. Наказ Порядок Держстандарту Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 2001.07.09 № 329/32 "Про затвердження Порядку проведення робіт з сертифікації засобів забезпечення технічного захисту інформації загального призначення"

37. Наказ Порядок Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 2001.12.24 № 76 "Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах" ,

38. ДНАОП 0.00-1.31-99 "Правила охорони праці під час експлуатації електронно-обчислювальних машин". Затверджені наказом Держнаглядохоронпраці від 10 лютого 1999 року № 21 // База даних "Ліга: Закон Professional"

39. ДНАОП 0.00-1.31-99 "Правила охорони праці під час експлуатації електронно-обчислювальних машин". Затверджені наказом Держнаглядохоронпраці від 10 лютого 1999 року № 21 // База даних "Ліга: Закон Professional"

40. ДСанПіН 3.3.2.007-98 "Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин". Затверджені постановою Головного державного санітарного лікаря України від 10 грудня 1998 р. № 7.

41. Перелік Державної митної служби від 2004.06.02 № 41/16-24-2838-ЕП "Щодо переліку технічних засобів захисту інформації"

42. Правила Мінфіну України від 2004.07.20 № 466 "Про забезпечення захисту інформації шляхом обмеження доступу до приміщень, у яких розміщене серверне та комутаційне обладнання"

43. Наказ Держбуду України від 2002.03.26 № 58 "Про затвердження державних стандартів технічного захисту інформації»

Інші законодавчо-нормативні видання

44. Резолюція Ради ЄС від 1995.01.17 №96/3 329/01 “Про законний моніторинг телекомунікацій”.

45. Конвенція Ради Європи від 2001.11.23 “Про кіберзлочинність”.

46. Доктрина информационной безопасности Российской Федерации. Утверждена

Президентом РФ 2000.09.09. —М., 2000.

47. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по информации. — М., 1992.

Підручники та навчальні посібники Основна література

48. Богуш В. М. Теоретичні основи захищених інформаційних технологій : навч. посібник / В. М. Богуш, О. А. Довидьков, В. Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.

49. Богуш В. М. Інформаційна безпека : термінологічний навч. довідник / В. М. Богуш, В. Г. Кривуца, А. М. Кудін; за ред. Кривуци В. Г. – К.: ООО «Д.В.К.», 2004. – 508 с.

50. Бурячок В. Л. Політика інформаційної безпеки: навч. посібник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко / за заг. ред. докт. техн. наук, проф. В. О. Хорошка. – К.: ПВП «Задруга», 2014. – 134 с.

51. Гуцалюк, М. В. Організація захисту інформації : навч. посібник. – 2-у вид., перероб. і доп. – К. Альтепрес, 2011. – 308 с.

52. Задірака В. К. Комп’ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях : навч. посіб. / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С. Олексюк – Київ-Тернопіль: Підручники і посібники, 2007. – 272 с.

53. Мухачев В. А. Методы практической криптографии / В. А. Мухачев, В. А. Хорошко. – К.: ООО «Полиграф-Консалтинг», 2005. – 215 с.

Додаткова література

54. Інформаційна безпека: сутність та проблеми (матеріали круглого столу). — Запоріжжя, 1998. – 23 с.

55. Жидецький, В.Ц. Охорона праці користувачів комп’ютерів / В.Ц.Жидецький. — Львів : Афіша, 2000.— 176 с.

56. Система забезпечення інформаційної безпеки України // Національна безпека і оборона. - 2001. - № 1. - С. 16-28

Статті, монографії

57. Актуальні проблеми інформаційної безпеки України. Аналітична доповідь УЦЕПД ім. Разумкова // Національна безпека і оборона. —К.: 2001. —№1. — С.2-59.

58. Александрова, Н. Системы защиты корпоративных сетей и аутентификации пользователей при помощи смарт-карт / Н.Александрова, В.Пузырин // Конфидент. —

1998. — № 4. — С. 30-32.

59. Балакшин, Е.В. Опыт работы с межсетевым экраном FireWall-1 / Е.В.Балакшин, С.В.Хлупнов // Конфидент. — 1999. — № 2 . — С. 54-59.

60. Баранов, А. Информационный суверенитет или информационная безопасность? / А.Баранов // Національна безпека і оборона. — К.:2001. — С.70-76.

61. Березин, А. С. Защита информация в открытых сетях / А.С.Березин, В.И. Прчиков // Корпоративные системы. — 2001. — № 1. — С. 65-69.

62. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки : монографія**.** – К.: НАУ, 2013. – 432 с.

63. Вэк Дж. Безопасность корпоративной сети при работе с Интернетом. Введение в межсетевые экраны / Дж. Вэк, Л. Карнахан // Конфидент. — 2000. — № 4-5. — С. 48-55.

64. Дешко, А. І. Проблеми організації єдиного інформаційного простору України / А.І.Дашко, А.Є.Слівак // Науково—технічна інформація. — К.:2000. — №3. — С. 14-18.

65. Конявский, В.А.. Понятия «документ» и «информационная технология», их базовые свойства. / В.А.Конявский // Безопасность информационных технологий. — 2004. — №2. — С. 16-19.

66. Лазарев, Г. Захист інформації в інформаційно-телекомунікаційних системах / Г.Лазарев // Національна безпека і оборона.— К.: 2001. — №1. — С. 80-83.

67. Серго, А.Г. Правовые аспекты электронного документооборота / А.Г.Серго // Безопасность информационных технологий. — 2014. — №2. — С. 22-30.

68. Фомін, В. О. Сутність і співвідношення понять «інформаційна безпека», «інформаційна війна» та «інформаційна боротьба»/ В.О.Фомін, А.О.Рось // Наука і оборона. – К.:1999. –№4. – С. 23-32.

Інтернет-видання

69. Апухтін, С. Інформаційна безпека як засіб протидії кіберзлочинності / С. Апухін [Електронний ресурс]. – Режим доступу: http://www. crime-research.ru. – Заголовок з екрану.

70.Баричев, С. Криптография без секретов / С. Баричев [Електронний ресурс]. – Режим доступу: http://athena.vvsu.ru/docs/science/crypt/barichev/ crypto.htm? – Заголовок з екрану.

71.Гриняев, С. И. Информационный терроризм: предпосылки и последствия / С.И.Гриняев [Електронний ресурс]. – Режим доступа: http://www.e-journal.ru/p_besop-stl9.html. - Заголовок с экрана.