**Курсова робота**

**на тему: «Загрози безпеки інформації»**

**ЗМІСТ**

**ВСТУП……………………………………………………………………………3**

**Розділ 1. Загальні положення про захист інформації………………………5**

1.1.Інформаційна безпека……………………………………………..………….5

1.2.Законодавчі вимоги і регулювання інформаційної безпеки……………….9

**Розділ 2. Характеристика загрози безпеки інформації……………………13**

2.1. Характеристика загроз безпеки інформації…………………………...….13

2.2. Класифікація загроз інформаційній безпеці……………………………..14

2.3. Джерела загроз……………………………………………………………..17

**Розділ 3. Сучасний стан інформаційної безпеки. Проблеми захисту комп’ютерної інформації…………………………………………………….20**

**ВИСНОВКИ…………………………………………………………………….26**

**СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ………………………………28**

**ВСТУП**

**Актуальність теми.** В умовах глобальної конкуренції держав за сфери впливу посилилась боротьба між різними суб ̓єктами міжнародних відносин за панування над свідомістю окремих соціальних груп та цілих на- родів. ….

**Мета і завдання дослідження.** Метою курсової роботи є  полягає у визначенні заходів забезпечення інформаційної безпеки у політичній, економічній, науки і … безпеки; розглянути характеристику загроз безпеки інформації ; дослідити класифікацію загроз інформаційній безпеці; проаналізувати **сучасний стан інформаційної безпеки.**

**За об'єкт дослідження** взято систему інформаційної безпеки як … безпеки інформації.

**Методи дослідження.** ….

**Практичне значення одержаних результатів** полягає в тому, що сформульовані в ..

**Структура та обсяг курсової роботи.** Курсова робота складається зі вступу, трьох розділів, підрозділів, додатків, висновків та списку використаних джерел. Загальна кількість сторінок - 30.

**Розділ 1. Загальні положення про захист інформації**

**1.1.Інформаційна безпека**

Інформаційна безпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави. Інформаційна безпеки, з одного боку, передбачає забезпечення якісного все- бічного інформування громадян та вільного доступу

до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, …..

Таким чином, …

**1.2.Законодавчі вимоги і регулювання інформаційної безпеки**

Інформаційна безпека в правовому вимірі є невід’ ємною складовою сучасної системи управління на шляху до правової держави і суттєвим чинником формування громадянського суспільства та входить до ширшого розуміння питань національної безпеки загалом.

За таких умов законодавча невизначеність щодо основних параметрів інформаційної безпеки, існуючі протиріччя та прогалини у правозастосовній практиці в цій сфері ускладнюють внутрішні трансформаційні перетворення та інтеграцію України в світові цивілізаційні процеси.

Зокрема, Законом України “Про інформацію” (ст. 6) передбачене створення загальної системи охорони інформації, однією зі складових якої повинно стати визначення державою правил віднесення відомостей до відповідної категорії інформації [5, с. 9].

Отже, інформаційну безпеку можна розглядати як елемент або підсистему національної безпеки. Національне законодавство України надає великого значення інформаційній складовій національної безпеки. Так, норма ч. 1 ст. 17 Конституції України встановлює, що “захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу” [6]. У цьому контексті інформаційна безпека розглядається … безпеки України, закони України, міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, а також підзаконні нормативно-..

**Розділ 2. Характеристика загрози безпеки інформації**

**2.1. Характеристика загроз безпеки інформації**

Незважаючи на те що поняття загрози неодноразово наводилося в різних доктринальних і нормативно-правових джерелах, досі немає єдиного підходу до визначення його змісту й ролі в теорії безпекознавства. Зокрема, А. Анто- нов і В. Балашов визначають загрозу як процес настання таких змін у стані особи, суспільства й держави, що оцінюються ними як здатні створити перешкоди або унеможливити реалізацію їхніх інтересів [11, с. 48]. Разом із тим слово «за- гроза» в словнику С. Ожегова с. означає можливу небезпеку, тому припускає не лише процес настання змін, а й можливість їх настан- ня. Під загрозою також розуміють «можливість або неминучість виникнення чогось небезпеч- ного, прикрого, тяжкого для кого-, чого-небудь», «те, що може заподіювати яке-небудь зло, якусь неприємність».

….ся загрозам, що виникають у зв’язку з інформацією, яка становить загрозу морально-психічному здоров’ю дітей та підлітків. На території СНД, за даними деяких провайдерів, еротика і порнографія складає не менше третини всього ринку …

**2.2. Класифікація загроз інформаційній безпеці**

Загрози національній безпеці можуть бути класифіковані за різними підставами, що висвітлює їх складну та багатошарову систему. Зокрема, у науковій політологічній думці загрози національній безпеці класифікуються за місцем знаходження джерела – зовнішні та внутрішні; за масштабами можливих наслідків – загальнонаціональні, регіональні, локальні, пооди- нокі; за ступенем сформованості – потенційні, реальні; за ступенем суб’єктивного сприйнят- тя – завищені, занижені, мінімальні, умовні, адекватні; за характером виникнення – загрози природного, техногенного й соціального характеру; за сферами життєдіяльності – загрози в економічній, політичній, оборонній, міжнарод- ній, соціальній, інформаційній, науково-технічній, екологічній, культурній і духовній сферах тощо.

М. Литвин і В. Кохан, досліджуючи питання внутрішньої безпеки, пропонують вирізняти загрози національній безпеці України у сферах політики, економіки, у соціальній і військовій сферах, у сферах екології, культури, освіти і просвітництва, боротьби зі злочинніс- тю, а також загрози, що … лежить характерне для глобалізації «відтериторіювання» явищ і процесів, які функціонують у тран- скордонному суспільному просторі, відірвані від територіальної локалізації.

Таким чином, …

**2.3. Джерела загроз**

Фактично, реалізація захисту має дві частини: код і настроювання (setup). Код – це програми в довірчій обчислювальній базі (в комплексі засо- бів захисту). Настроювання – це всі дані, які управляють операціями цих програм: списки контролю доступу, членство в групі, користувацькі паролі, ключі шифрування і т.д.

Задача реалізації захисту повинна бути спроможна протидіяти загрозам, які зустрічаються в трьох основних формах:

- погані (помилкові або ворожі) програми;

- погані (ворожі) агенти – користувачі (або програми), які надають хо- рошим, але легковірним програмам свідомо помилкові команди;

- погані агенти, які підключаються до комунікацій і заповнюють їх своїми повідомленнями.

У загальному випадку існують чотири стратегії захисту.

1. Нікого не впускати. Це повна ізоляція. Вона забезпечує найкращий захист, але перешкоджає використанню інформації або послуг від інших, і передачі їх іншим користувачам. Це непрактично для всіх.

2. Не впускати порушників. Програми всередині цього захисту можуть бути … Сил України, так і у впливі на цю діяльність.

Таким чином, ..

**Розділ 3. Сучасний стан інформаційної безпеки. Проблеми захисту комп’ютерної інформації**

Широке використання інформаційних технологій у всіх сферах життя суспільства робитьдосить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних від злочинних зазіхань зловмисників.

Концентрація інформації в комп'ютерах (аналогічно концентрації готівки в банках) змушує одних усе більш підсилювати пошуки шляхів доступу до інформації, а інших, відповідно, підсилювати контроль над нею з метою захисту.

Складність створення системи захисту інформації визначається тим, що дані можуть бути викрадені з комп'ютера (скопійовані), одночасно залишаючись на місці. Цінність деяких даних полягає у володінні ними, а не в їх знищенні або зміні.

Забезпечення безпеки інформації – справа дорога, і не стільки через витрати на закупівлю або установку різних технічних або програмних засобів, скільки через те, що важко кваліфіковано визначити межі розумної безпеки і відповідної підтримки системи в працездатному стані.

Сьогодні …

**ВИСНОВКИ**

Підсумовуючи вищевикладене слід зазначити, що інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема політична обстановка у світі; внутріш- ньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо.

Загрози ….

**СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ**

1. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко.URL: http://www.crime-research.iatp.org.ua/library/strateg.htm (дата звернення: 26.11.2020 р.).

2. Ларина Е. С. Кибервойны ХХІ века: о чем умолчал Эдвард Сноуден / Елена Ларина, Владимир Овчинский. М.: Книжный мир, 2014. 349 c.

3. Манойло А.В. Проблемы и перспективы исследования информационно-психологических технологий разрешения международных конфликтов. Право и политика, 2008. № 3. С. 592-598.

4. Україна-2020: зовнішньополітичні виклики та можливості наступного десятиріччя. Український інститут публічної політики. URL: http://uipp.org.ua/uploads/news\_ message/at\_file\_uk/0070/38.pdf. (дата звернення: 26.11.2020 р.).

5. Мастяниця Й. У. Захист інформаційних ресурсів України: проблеми і шляхи їх розв’язання / Й. У. Мастяниця, О. В. Соснін, Л. Є. Шиманський; Національний ін-т стратегічних досліджень. К., 2000. 99 с.

6. Конституція України: прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. із змінами від 8 груд. 2004 р. / Офіц. вид. – К.: Видавн. Дім “Ін Юре”, 2006.

7. Скакун О. Ф. Теория государства и права / О. Ф. Скакун. – Х.: Консум, Ун-т внутр. дел, 2000. С. 45.

8. Юридична енциклопедія: в 6 т. / Ред. кол.: Ю. С. Шемшученко (відп. ред.) та ін. – К.: Укр. енцикл. імені М. П. Бажана. –1999. Т. 2. 744 с.

9. Ліпкан В.А. Національна безпека України: Навч. посіб. 2-ге вид. К., 2009.

10. Ярочкин В.И. Информационная безопасность: Учеб. пособие для студ. непрофильных вузов. М., 2000.

11.Антонов А.Б. Основы обеспечения безопас- ности личности, общества и государства : [учебное пособие] / А. Антонов, В. Балашов. М. : Институт защиты предпринимателя, 1996. С. 36–55.

12. Горбулін В.П. Засади національної безпеки України / В. Горбулін, А. Качинський. К. : Інтер- технологія, 2009. 272 с.

13. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. No 514/2009.URL: //www.president.gov.ua/documents/9570.html (дата звернення: 26.11.2020 р.).

14.Литвин М.М. Умови та фактори внутрішньої загрози національній безпеці України / М. Литвин, В. Кохан [Електронний ресурс].URL: plesetsk-info.ru/uchebnoe-posobie/umovi-ta-faktori- vnutrshno-zagrozi-natconalni-bez.

15. Ліпкан В.А. Національна безпека України : [навчальний посібник] / В. Ліпкан. К. : КНТ, 2009. 576 с.

16. Хусаинов М.И. Современные подходы к классификации транснациональных угроз безопасности / М. Хусаинов. Вестник Военного университета, 2010. № 1 (21). С. 65–70.

17. Світлична В.Ю. Інформаційна безпека: ба- гатогранність сутності, види загроз та шляхи забез- печення / В. Світлична, Т. Світлична // Науково- технічний збірник. Х. : ХНАМГ, 2013. № 109. С. 360–369.

18. Горбулін В. П. Інформаційні операції та без- пека суспільства: загрози, протидія, моделювання : [монографія] / В. Горбулін, О. Додонов, Д. Ланде. К. : Інтертехнологія, 2009. 164 с.

19. Сопілко І.М. Інформаційні загрози та безпека сучасного українського суспільства / І. Сопілко / Юридичний вісник, 2015. № 1 (34). С. 75–80.

20. Куцька О.М. Особливості інформаційно-пси- хологічного впливу Російської Федерації напередод- ні та початковому етапі антитерористичної опера- ції на сході України / О. Куцька. Інформаційна безпека людини, суспільства, держави. 2017. № 1(21). С. 180–190.

21. Снитко О.С. Проекти тотального зомбування в інформаційному просторі України / О. Снитко. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С. 207–215.

22. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. К І І В і П НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

23. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016) [Online tool]. Available at : https:// cio.com/article/ 3153706/security/4-information-security-threats-that- will-dominate-2017.html. (дата звернення: 26.11.2020 р.).

24. Живко З. Інформаційні загрози: суть і про- блеми / З. Живко, М. Живко / Безпека та захист інформації в інформаційних системах : тези доповідей ІІ міжнародної НПК. К., 2017. C. 116–118.

25. Левченко Ю.О. Проблеми протидії інформаційній окупації в умовах гібридної війни. Інформаційна безпека в умовах гібридної війни: Міжнародна науково-практична конференція (м. Хмельницький, 16–17 листопада 2017 р.). Хмельницький : МВС УКРАЇНИ, 2017. 50 с.

26. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.