МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

ЗАВДАННЯ ТА МЕТОДИЧНІ ВКАЗІВКИ
до виконання контрольної роботи
для студентів напряму підготовки (спеціальності)
6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»
денної форми навчання

Обговорено і рекомендовано
на засіданні кафедри
кібербезпеки та математичного моделювання
Протокол № 5
від «18» жовтня 2017 р.

Чернігів ЧНТУ 2017

Інформаційна безпека держави. Завдання та методичні вказівки до виконання контрольної роботи для студентів напряму підготовки (спеціальності) 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» денної форми навчання / Укл.: Гур'єв В.І. – Чернігів: ЧНТУ, 2017. – 25 с.

Укладачі: Гур'єв Володимир Іванович, кандидат технічних наук, доцент, професор кафедри кібербезпеки та математичного моделювання

Рецензент: Мехед Дмитро Борисович, доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук, доцент

ЗМІСТ

ПЕРЕДМОВА

Навчальна дисципліна «**Інформаційна безпека держави**» цілком відповідає вимогам підготовки достатньо компетентних спеціалістів в галузі інформаційної безпеки. Проте, ця дисципліна має бути посилена і підкріплена завданнями, тестами та іншими вправами, котрі забезпечували б органічний зв'язок теорії з практичною діяльністю і дали б змогу студентам більш глибоко засвоювати навчальну дисципліну та накопичувати необхідні компетенції.

Запропоновані завдання включають методичні вказівки до виконання, варіанти завдань, критерії оцінювання. За допомогою контрольної роботи та запропонованих завдань досягається більш глибоке опанування теорії, що здійснюється за допомогою розвитку логічного мислення через виконання індивідуальних завдань та дає змогу студентам осмислити нові для них поняття. Завдання для роботи скомпоновані відповідно до робочої програми дисципліни, що полегшує і робить більш зручною організацію навчального процесу і викладачам, і студентам.

Завдання для контрольної роботи студентів можуть використовуватися як для аудиторної, так і домашньої роботи. Вони спрямовані на розвиток аналітичних здібностей, а також уміння користуватися теоретичними посиланнями у вирішенні практичних завдань та вміння користуватися програмним забезпеченням і спеціальною літературою.

Під час виконання контрольної роботи студенти повинні ознайомитися та вивчити лекційний матеріал, запропонований викладачем. Основою для вивчення є літературні джерела, наведені в даній розробці. За наявності незрозумілих питань студентам рекомендується звернутись за консультаціями до викладача з метою отримання всіх необхідних пояснень щодо організації контрольної роботи та пошуку додаткових літературних джерел. Викладачем надаються додаткові роз'яснення та індивідуальні консультації для підвищення компетентності студентів та розширення спектру їх знань.

КРИТЕРІЇ ОЦІНЮВАННЯ КОНТРОЛЬНОЇ РОБОТИ

З даного курсу контрольна робота проводиться у формі виконання індивідуального завдання по конкретному варіанту.

Для *захисту контрольної роботи* студент повинен відповісти на три питання за вибором викладача по різних частинах індивідуального варіанта. В тому випадку, коли студент відповідає на всі питання без помилок (або з несуттєвими помилками), контрольна робота вважається захищеною. Якщо при відповіді студент допускає грубі помилки, або питання виконані менш ніж на половину, то робота вважається незахищеною.

Шкала оцінювання знань студентів при виконанні контрольної роботи

Рівень виконання контрольної роботи	**Кількість балів**	
- усі питання розглянуті повністю і правильно; - посилання на літературу здійснено правильно; - показано вміння самостійно формулювати висновки; - присутній творчий підхід при виконанні роботи; - використано новітні інформаційні технології.	9…	10
- питання розглянуті повністю, але допущені незначні помилки; - частина матеріалу викладена не аргументовано; - у висновках містяться помилки та недоречності.	6…	8
- питання розглянуті , але містять грубі помилки; - робота виконана не у повному обсязі та допущено значні помилки; - не сформульовані висновки за результатами роботи.	3…	5
- питання розглянуті частково і неякісно; - висновки не зроблені; - вимоги по оформленню роботи не виконані.	0…	2

Оцінка за виконання контрольної роботи, додається до підсумкової модульної оцінки, переведеної за шкалою ECTS.

Вибір варіанту контрольної роботи.

Варіант контрольної роботи видається студенту викладачем *згідно порядкового номеру в списку академічної групи або за власним бажанням.*

ВАРІАНТИ КОНТРОЛЬНОЇ РОБОТИ

1. Актуальні проблеми інформаційної безпеки в Україні і шляхи їх вирішення.
2. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення.
3. Правові аспекти і законодавче забезпечення захисту інформації в Україні.
4. Характеристика основних видів національної безпеки України.
5. Проблеми захисту персональних даних в Україні.
6. Стратегія кібербезпеки України.
7. Стан тенденції та проблеми захисту інформації в інформаційних системах.
8. Інформаційна війна: сутність, методи та засоби ведення.
9. Захист банківської таємниці в Україні.
10. Державна таємниця та система її охорони.
11. Класифікація загроз інформації сучасних інформаційних систем та мереж.
12. Класифікація каналів витоку інформації в сучасних інформаційних системах.
13. Рекомендації по організації системи захисту інформації в комерційних структурах.
14. Основи державної інформаційної політики в сфері захисту інформації.
15. Інформаційні системи та технології як об'єкти інформаційної безпеки.
16. Роль і місце інформаційної безпеки в загальній системі національної безпеки держави.
17. Інформаційні системи та технології як об'єкти інформаційної безпеки.
18. Основи нормативно-правового забезпечення захисту інформації в комп'ютерних системах.
19. Інформаційна безпека в Internet: кримінологічний аспект.
20. Особливості розвитку Internet в Україні і інформаційна безпека.
21. Безпека інформації в комп'ютерних системах та можливі підходи до її експертної оцінки.
22. Боротьба з комп'ютерними правопорушеннями : проблеми і шляхи їх вирішення.
23. Інформаційна боротьба, інформаційна війна і інформаційна зброя.
24. Психологічна війна: підготовка, ведення, методологія оцінки ефективності.
25. Обмеження свободи слова і доступу громадян до інформації.
26. Негативні чинники впливу на інформаційну безпеку у сфері суспільної моралі.
27. Правопорушення у сфері інформаційних технологій .
28. Правові засади забезпечення інформаційної безпеки держави.

29. Основи державної політики у сфері забезпечення інформаційної безпеки держави.
30. Інститути громадянського суспільства як суб'єкти забезпечення інформаційної безпеки.
31. Юридична відповідальність за правопорушення у сфері забезпечення інформаційної безпеки.
32.Система попередження витоку персональних даних мережевими каналами.
33.Основні напрями забезпечення безпеки інформації підприємства.

Приклад виконання контрольної роботи

Міністерство освіти і науки України

Чернігівський національний технологічний університет

Факультет життєдіяльності, природокористування і туризму

Кафедра кібербезпеки та математичного моделювання

Контрольна робота

з дисципліни «Інформаційна безпека держави»

На тему: "*Боротьба з комп'ютерними правопорушеннями, проблеми і шляхи їх вирішення*"

Виконав:

Ст. групи КБ-161

Перевірив:

Професор В. І. Гур'єв

Чернігів, 2016

Зміст

ВСТУП

Як і будь-яке соціальне явище інформатизація має не тільки позитивну для суспільства сторону, але і зворотну, негативну: використання комп`ютерних технологій в протиправних, антисоціальних, злочинних цілях. Дослідження свідчать, що комп`ютерна злочинність у світі має тенденцію до зростання. Особливу небезпеку в складі комп`ютерних правопорушень мають злочини, що вчиняються організованими угрупуваннями. Проникнення організованих злочинних формувань у кіберпростір - комп`ютерний інформаційний простір, породило зміну засобів і способів вчинення деяких традиційних злочинів (крадіжки, шахрайства, тероризм, шпигунство, вимагательство, політичний шантаж, недобросовісна конкуренція тощо).

З того часу коли в 1988 році вірус-черв'як (Morris Worm) паралізував половину комп'ютерів, що працювали в мережі Internet, Internet залишається не тільки засобом передачі інформації в науковій, оборонній та інших сферах, але й став глобальною електронною мережею, яка втілена в усі аспекти нашого життя як вдома, так і на роботі. Атаки в мережі, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, корпоративне шпигунство та поширення дитячої порнографії - ось тільки деякі зі злочинів, що вчиняються в мережі Internet.

Такі протиправні діяння вже сьогодні складають для нашої держави, як і для багатьох інших країн світу, певну суспільну небезпеку, реально загрожуючи інформаційній безпеці - складовій національної безпеки. Національна інфраструктура держави вже сьогодні щільно пов'язана з використанням сучасних комп'ютерних технологій. Щоденна діяльність банківських та енергетичних систем, керування повітряним рухом, транспортна мережа, навіть швидка медична допомога перебувають у майже повній залежності від надійної і безпечної роботи автоматизованих електронно-обчислювальних систем.

На сучасному етапі розвитку нашого суспільства прогнозується подальше зростання залежності життєдіяльності національної інфраструктури від процесів інформатизації та входження України в єдиний інформаційний простір, поширення криміногенних процесів, пов'язаних з протиправним використанням комп'ютерних технологій.

Вітчизняна та світова практика свідчить, що число клієнтів Internet продовжує бурхливо зростати, а разом із цим зростає і кількість атак, яких щодня зазнають комп'ютерні системи із зовнішнього середовища. За статистикою Американського Інституту Комп'ютерної Безпеки (Computer Security Institute), збитки від злочинів, що вчиняються за допомогою комп'ютерних технологій, з кожним роком збільшуються.

Разом із поширенням впровадження сучасних інформаційних технологій в Україні постійно зростає загроза як для державних комп'ютерних систем, так і для приватних організацій та окремих громадян. Особливої актуальності проблема кіберзлочинності набула в наш час.

КІБЕРЗЛОЧИННІСТЬ

Термін "кіберзлочин" молодий і утворений сполученням двох слів: кіберпростір і злочин. Термін кіберпростір (у вітчизняній літературі частіше зустрічаються терміни "віртуальний простір" або "віртуальний світ") позначає інформаційний простір, що моделюється за допомогою комп'ютера, у якому існують визначеного роду об'єкти або символьне уявлення інформації - місце, де діють комп'ютерні програми і переміщуються дані. Використання цього терміна поширене у світовій науковій літературі та вживається автором не як юридична категорія, а як визначення соціального та технічного феномена. Термін "кіберзлочини" в подальшому використовуватиметься і як синонім термінів "транснаціональні комп'ютерні злочини", "злочини, що вчиняються за допомогою мережі Internet". Під терміном "кіберзлочини" будемо розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Internet на інформацію в комп'ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особі, політичним, трудовим, майновим та іншім правам і свободам громадян.

БОРОТЬБА З ПРАВОПОРУШЕННЯМИ

Боротьба зі злочинністю у сфері використання автоматизованих електронно-обчислювальних систем (далі - комп'ютерні злочини), вже сьогодні є одним із важливіших державних завдань. Для того, щоб ця боротьба була максимально ефективною, безумовно, необхідно дослідження цієї ще нової для нашого суспільства форми злочинності, її складових, виявлення відповідних закономірностей і тенденцій, а також глибоке вивчення організаційно-правових та інших можливих заходів, що перешкоджають її поширенню, розробка заходів попередження і розслідування таких видів злочину.

При недостатній практиці розслідування комп'ютерних злочинів (далі - КЗ) і судового розгляду таких справ, необхідних для розробки їхньої криміналістичної характеристики, можливе застосування порівняльного аналітичного і прогностичного підходів.

Джерелами їх здійснення є:

- ❖ Стан, структура, характеристика КЗ в країнах, де поширені ці діяння і розроблено засоби боротьби з ними;
- ❖ Досвід правового регулювання боротьби з цим видом злочинів;
- ❖ Практика виявлення, розслідування і профілактики;
- ❖ Діяльність правоохоронних структур щодо збору, накопичування та аналізу інформації, що стосується КЗ.

Стан КЗ характеризується наявністю діянь, предметом зазіхання яких є комп'ютерна інформація, її носії, або протиправними діями, для здійснення яких комп'ютер використовується як знаряддя.

ВИДИ ПРАВОПОРУШЕНЬ

До сучасного складу КЗ включаються все нові види протиправних діянь, хоч і не скрізь досить оформлені в правовому відношенні. Так, на сьогодні до цього переліку вже відносять:

❖Несанкціоноване проникнення в автоматизовані електронно-обчислювальні системи;

❖ Розкрадання системного і прикладного програмного забезпечення;

❖Несанкціоноване копіювання, модифікацію або знищення комп'ютерної інформації;

❖Блокування комп'ютерної інформації, шантаж та інші методи комп'ютерного тероризму;

❖ Комп'ютерне шпигунство;

❖ Підробку і фальсифікацію комп'ютерної інформації;

❖ Розробку і поширення комп'ютерних вірусів і програмних закладок;

❖ Несанкціонований перегляд або розкрадання інформації з банків даних і баз знань;

❖ Халатну недбалість при розробці, створенні автоматизованих електронно - обчислювальних систем і програмного забезпечення, що призводить до тяжких наслідків і втрати інформації;

❖Механічні, електричні, електромагнітні та інші види впливу на автоматизовані електронно-обчислювальні системи;

❖ Мережеве шахрайство;

❖ Шахрайство з використанням пластикових платіжних карток;

❖Використання глобальної інформаційної мережі Intemet для вчинення віддалених атак проти електронно-обчислювальних систем.

Мабуть, цей перелік не є повним, а буде з часом поповнюватися, але щодо структури КЗ в узагальненому вигляді можна дотримуватися рекомендацій, що були надані ще в 1990 р. Європейським комітетом з проблем злочинності Ради Європи для включення в законодавство європейських країн списку протиправних діянь у сфері комп'ютерної інформації:

КОМ'ПЮТЕРНЕ ПІРАТСТВО ЯК ВИД ПРАВОПОРУШЕНЬ

Піратство у сфері інтелектуальної власності щодо програмного забезпечення (ПЗ) займає третє місце в світі по прибутковості після наркотиків і зброї, що і робить його одним з самих небезпечних видів комп'ютерних злочинів, включених в міжнародну класифікацію (вид QR – незаконне копіювання).

Комп'ютерне піратство (КП) набуло поширення в світі на рубежі 70-80-их років майже одночасно з появою ПК. До їх появи ПЗ звичайно знаходилося у розпорядженні виробників ЕОМ і передавалося користувачам в комплекті з ЕОМ. Виникнення ажіотажного попиту на різноманітні програми саме для ПК зумовило появу комп'ютерного піратства (від англ. "piracy"), як одного з основних видів правопорушень щодо авторських та суміжних прав власників ПЗ

Нажаль, Україна входить до переліку країн з високим рівнем КП (біля 85% за різними оцінками), що зумовлює актуальність проблеми, що розглядається.

Різні аспекти проблеми протидії КП розглядали багато вітчизняних (В. І. Жуков, В. Ландик, В. Негрескул, М. В. Селіванов, К. В. Титуніна та ін.) та закордонних (І. Маміофі, Л. І. Подшибихіна, Л. С. Сімкін, О. Ревинський, Дж. Фокс та ін.) науковців.

Проте, навіть однозначного визначення поняття КП дотепер не існує.

К. Титуніна визначає, що "під комп'ютерним піратством слід розуміти копіювання або поширення комп'ютерних програм, захищених авторським правом, без згоди на те власника авторських прав" .

На думку А. Родзевича під цим терміном слід розуміти "дії, які будь-яким способом порушують авторські права на програмне забезпечення" .

М. Селіванов взагалі вважає, що "термін "піратство" є не юридичним, а сленговим висловлюванням і тому має бути виключений з тексту Закону".

В Законі України "Про авторське право і суміжні права" в редакції від 11 липня 2001 р. визначено, що: "піратство у сфері авторського права і (або) суміжних прав – опублікування, відтворення, ввезення на митну територію

ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ З КОМПЮТЕРНИМИ ПРАВОПОРУШЕННЯМИ

У січні 2013 року в Гаазі відкрився Європейський центр боротьби з кіберзлочинністю (ЕС3). Завдання ЕС3 - присікати дії організованих злочинних мереж. На даний момент об'єкти уваги ЕС3 обмежені трьома: онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи.

22 вересня 2014 року Європейський центр боротьби з кіберзлочинністю Європолу (ЕС3) та Європейська банківська федерація (ЄБФ) підписали Меморандум про взаєморозуміння, який відкриває шлях для активізації співпраці між правоохоронними органами та фінансовим сектором в ЄС.

Для протистояння кібершахраям в світі створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюються, а технічні можливості посилюються. Останній приклад – Європейський центр боротьби з кіберзлочинністю, який запрацював на початку 2013 року. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній. За деякими оцінками, через кіберзлочинців щорічно світова економіка втрачає $ 114 млрд, повідомляє РБК. А США оцінили свої збитки за всі роки існування глобальної мережі у $ 400 млрд. Це у три рази більше щорічних витрат на освіту.

З огляду на складність проблеми, Рада Європи підготувала і опублікувала проект Конвенції щодо боротьби зі злочинами у кіберпросторі, який планується остаточно прийняти у вересні 2001 року. Реалізуючи положення цього документа, на національному рівні необхідна гармонізація кримінального законодавства з урахуванням рекомендацій Ради Європи і норм міжнародного права. Така необхідність викликана тим, що часто при вчиненні таких видів злочинів об’єкт і суб’єкт знаходяться в різній юрисдикції, існує дуже великий ризик того, що злочинці будуть здійснювати свої протиправні дії з території держав, де такі діяння не віднесено до кримінальних. Тому, підписання і прийняття Україною запропонованої Конвенції щодо попередження кіберзлочинів сприятиме зміцненню міжнародного співробітництва в боротьбі з цими видами злочинів.

Криміногенна ситуація у сфері використання автоматизованих електронно-обчислювальних систем потребує комплексного підходу стосовно вирішення проблем попередження і розслідування КЗ. Застосування системи заходів завжди є більш ефективним, ніж вплив на злочинність окремими діями. Коли при розробці заходів дотримується комплексний системний підхід, що включає в себе різні рівні, тоді отримання позитивних результатів стає реальним.

Комплекс заходів щодо боротьби з КЗ повинен спиратися на єдину державну політику в цій галузі. Для цього повинна бути розроблена науково обгрунтована програма, яка включатиме заходи державного, політичного, економічного, соціального, правового та іншого характеру.

Введення в дію з 1 вересня 2001 р. нового Кримінального кодексу України, прийняття до кінця 2001 року, нового Кримінально-процесуального кодексу України, а також приєднання України до Страсбургської Конвенції щодо попередження кіберзлочинів (Draft Convention on Cyber-crime) дуже важливий крок у вирішенні цих проблем та надання необхідних і ефективних кримінально-правових та процесуальних механізмів, спрямованих проти загрози поширення кіберзлочинів у сферах державного та приватного сектору економіки нашої держави.

Нарешті, задачею виняткової важливості для побудови національної системи боротьби з правопорушеннями, у сфері використання комп'ютерних технологій є проведення науково-дослідних робіт по вирішенню проблем попередження та розслідування кіберзлочинів та залучення у цю роботу широкого кола науковців та громадськості. Саме на це і спрямована діяльність відомого, як на Україні, так і за її межами, Центру дослідження проблем комп'ютерної злочинності, який функціонує на базі Web сайту www.crime-research.org. У липні місяці 2001 р. Центр дослідження проблем комп'ютерної злочинності увійшов до складу партнерів Національного центу підвищення кваліфікації фахівців у галузі боротьби з кіберзлочинами (National Cybercrime Training Partnership) - проекту, створеному під патронажем Міністерства Юстиції США з метою організації співробітництва з партнерами у рамках програми боротьби зі злочинністю в галузі високих технологій та був прийнятий до Міжнародної Асоціації Дослідників Злочинності - The International Association of Crime Analysts (I.A.C.A.).

Як ***висновок***, хочеться ще раз підкреслити, що проблема боротьби з комп'ютерними злочинами – це комплексна проблема. Злочини у галузі використання інформаційних технологій не піддаються результативному розслідуванню тими засобами і заходами, що були ефективні у минулому столітті, коли інформатизація нашого суспільства тільки починалась. Закони повинні сьогодні відповідати тим вимогам, що пред'являє сучасний рівень розвитку технологій, щоб відправлення правосуддя відбувалося у незалежності від того, чи був такий злочин вчинений за допомогою звичайних засобів або персонального засобу супутникового зв'язку та мережі Internet.

ЛІТЕРАТУРА

1) Боротьба з комп'ютерними злочинами –проблема транснаціонального масштабу/ [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/library/Cybercr.htm

2)Проблема боротьби із комп'ютерним піратством в Україні та шляхи її вирішення / [Електронний ресурс] – Режим доступу: http://user-master.org/stati-uroki/16-yuzeru/informatsionnaya-bezopasnost/59-problema-borotbi-iz-komp-yuternim-piratstvom-v-ukrajini-ta-shlyakhi-jiji-virishennya.html

3) Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. - //Економічна правда від 26 лютого, 2013року.

4) Европейский центр борьбы с киберпреступностью отчитался за первый год работы / [Електронний ресурс] – Режим доступу: http://www.interfax.ru/world/357250

5) Європейський центр боротьби з кіберзлочинністю Європолу і Європейська банківська федерація і об'єднують зусилля/ [Електронний ресурс] – Режим доступу: http://interpol.np.gov.ua/?p=2509

МЕТОДИЧНІ ВКАЗІВКИ ЩОДО СТРУКТУРИ РОБОТИ

Структура роботи охоплює: титульний аркуш; зміст; вступ, питання, що розкривають суть проблеми; висновки, список використаної літератури. Кожний елемент контрольної роботи обов'язково починається з нового аркуша.

Зміст роботи фактично відбиває план викладення обраної теми, в якому наводиться вся структура роботи з чіткими, конкретними формулюваннями питань.

Пропонується використовувати як фундаментальні підручники, словники, енциклопедії, монографії, так і довідники, статистичні збірки та періодичні видання.

Список літератури розміщується в кінці роботи. Він охоплює всі джерела, якими користувався автор (5-10 джерел). Оформлюється список літератури в алфавітному порядку, джерела також нумеруються для

здійснення посилань на них.

Таким чином, контрольна робота повинна бути підготовлена як цілісне закінчене дослідження з визначеної теми та розв'язанням практичного завдання, рівень виконання яких свідчить про глибоку теоретичну та практичну підготовку студента.

ВИМОГИ ДО ОФОРМЛЕННЯ КОНТРОЛЬНОЇ РОБОТИ

Методичні вказівки до оформлення контрольної роботи

Творчий підхід до написання контрольної роботи передбачає глибоке вивчення літератури з теми, оцінку різних трактувань питання, отримання аргументованих висновків.

Текст контрольної роботи слід викладати логічно, але при цьому не допускати простого переписування його з літератури. Наводячи цитати, формулюючи певні підходи, використовуючи запозичені статистичні матеріали з різних джерел, автор обов'язково повинен зробити посилання, а ці джерела назвати у загальному списку літератури.

Стосовно вимог до структури контрольної роботи кафедра подає такі рекомендації: загальний обсяг роботи повинен складати 15-20 сторінок тексту, який набирається на комп'ютері або пишеться від руки та оформлюється відповідним чином (див. нижче).

Відредагований текст контрольної роботи повинен бути надрукований на стандартних аркушах А4; шрифт 14 через 1,5 інтервали.

Посилання можуть бути подані на сторінках роботи, наприклад, наприкінці речення - [1, с.123], з вказівкою на порядковий номер літературного джерела у списку літератури та відповідно сторінку твору, що цитується. Також посилання можуть бути розташовані наприкінці сторінки, коли текст підкреслюється і друкується посилання меншим шрифтом - 10 через 1 інтервал. Студент може обрати будь-який варіант, однак пріоритетним є перший.

Рисунки та таблиці у контрольній роботі повинні бути правильно

оформлені та підписані. Назва рисунка розміщується під ним, назва таблиці - навпаки, їх нумерація здійснюється відповідно до глав. Наприклад, рисунок 1.3 - це третій малюнок у першій главі.

Робота оформляється на листах А4 з однієї сторони, поля: з лівого боку – 20 мм, з правого боку – 10 мм, зверху – 20 мм, знизу – 20 мм. Тема роботи повинна бути викладена акуратно, з детальними поясненнями кожного питання. Наприкінці роботи робиться висновок.

Вимоги до комп'ютерного набору контрольної роботи:

– текстовий редактор – WORD;

– гарнітура шрифту – Times New Roman;

– кегль шрифту (розмір) – 14; абзац – 1,25 см;

– міжрядковий інтервал – полуторний;

– розташування тексту роботи – вирівнювання по ширині;

– міжрядковий інтервал між заголовком (назвою розділу чи підрозділу) і текстом повинний дорівнювати 1 інтервалу.

Нумерацію сторінок слід починати з третьої (початок вступу) і до останньої, враховуючи додатки.

Повністю оформлена і виконана контрольна робота подається на кафедру в термін, що визначений у плані-графіку виконання контрольної роботи для перевірки її викладачем. Якщо робота виконана не вчасно без поважних причин, то студенту ставиться 0 балів («незадовільно») і він повинен виконати додатково один з варіантів, який вкаже викладач. Контрольна робота оцінюється після особистої співбесіди з викладачем. В разі зауважень з боку викладача, робота повинна бути доопрацьована в зазначений термін і подана на перевірку.

До підсумкового контролю допускаються лише студенти, що вчасно здали і захистили свою роботу.

Зразок титульної сторінки контрольної роботи наведено у додатку А.

Зразок оформлення літератури наведено в додатку Б.

Рекомендована література

Базова

1. Актуальні проблеми забезпечення національної безпеки України: Матеріали науково-практичної конференції / Київ. нац. ун-т внутр. справ.— К.: Текст, 2005. — 206 с. (Серія: Національна і міжнародна безпека).
2. Безпека інформації. Науковий журнал «Безпека інформації» засновано у 1995 році. Засновником та видавцем є Національний авіаційний університет.
3. Безпека резервного копіювання даних в хмарній системі збереження */Борис Геннадьевич Атаян, Татевик Араевна Багдасарян* // Безпека інформації. — 2016. - Том 22, № 2 (2016). С.119-122.
4. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
5. Глобалізація і безпека розвитку / [Білорус О. Г., Гончаренко М. О., Зленко В. А. та ін.]; НАН України, Київ. нац. екон. ун-т. - К.: КНЕУ, 2011. - 733 с.
6. Глобальные трансформации и стратегии развития: Монография. / Белорус 0., Лукьяненко Д. и др. - К.: Орияне, 2000. – 424 с.
7. Захист інформації. Науковий журнал «Захист інформації» засновано у 1999 році. Засновником та видавцем є Національний авіаційний університет.
8. Ліпкан В.А. Безпекознавство: Навчальний посібник. — К.: Вид-во Свроп. ун-та, 2003. — 208 с.
9. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення. — К.: Текст, 2010. — 180 с.
10. Ліпкан В.А. Національна безпека і національні інтереси України. — К.: КНТ, 2006. — 68 с (Серія: Національна і міжнародна безпека).
11. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України: Монографія. — К.: Текст, 2005. — 350 с
12. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України: Монографія. — К.: Текст, 2003. — 600 с.
13. Ліпкан В.А., Ліпкан О.С., Яковенко О.О. Національна і міжнародна безпека у визначеннях та поняттях. — К.: Текст, 2006. — 256 с
14. Ліпкан В.А. Управління системою національної безпеки України. — К.: КНТ, 2006. — 68 с (Серія: Національна і міжнародна безпека).
15. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : Навч. посіб. для вищих навч. закладів / Українська Академія держ. управління при Президентові України; Академія держ. податкової служби України. — К. : Преса України, 2010. — 304 с.
16. Проблеми національної та міжнародної безпеки України: Матеріали міжнародної науково-практичної конференції (Київ, 27 квітня 2007 р.) / Київ. нац. ун-т внутр. справ. — К.: Текст, 2007. (Серія: Національна і міжнародна безпека).
17. Про основи національної безпеки України: Закон України // Офіційний

Вісник України. — 2008. — № 29. — Ст. 1433.
18. СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ. Науковий журнал.
Тематика: інформаційна безпека, засоби захисту інформації
Засновники: Державний університет телекомунікацій.
19. Стратегія національної безпеки України // www.president.gov.ua
20. Указ президента України № 96/2016. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “ Про Стратегію кібербезпеки України” // www.president.gov.ua
21. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.
22. Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett- Packard Company.
23. Kiountouzis, E.A.; Kokolakis, S.A. Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4.

Допоміжна

1. Абрамов В.С. Коммерческая безопасность предприятий (теория и практика). — М.: АР-СИН ЛТД, 2008. — 76 с.
2. Актуальні проблеми інформаційної безпеки України. Аналітична доповідь УЦЕПД // Національна безпека і оборона. - К.: 2001. - №1. - С.2-59.
3. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / МВС України, Ун-т внут. справ - Х., 2010. -366с.
4. Гавловський В.Д, Голубев В.О., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері комп'ютерних технологій - Х.: Фоліо, 2002. - 284 с.
5. Кемп С. Роберт Легальный промышленный шпионаж: Бенчмаркинг бизнес-процессов: технологии поиска и внедрения лучших методов работы ваших конкурентов / пер. с англ. — Днепропетровск: Баланс-Клуб, 2004. — 416 с.
6. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії: Моногр. - К., - 2000. - 222 с.
7. Литвиненко О. Інформація і безпека // Нова політика. - 1998. - № 1. С 47.
8. Ліпкан В.А. Методологія формування правового поля забезпечення національної безпеки України // Держава і право. — 2002. — № 18. — С. 70 - 76.
9. СІПРІ 2003: Щорічник: озброєння, роззброєння та міжнародна безпека. — К.; Заповіт, 2004. — 652 с.
10. Шепелев М.А. Теорія міжнародних відносин: Підручник/' За ред. Д.Б. Табачника.- К.: Вища школа, 2004.- 622с.
11. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект. Фонд „Мир", 2003. — 640 с.
12. Указ президента України № 449/2014. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. “ Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України ” // www.president.gov.ua

Інформаційні ресурси

1. http://en.wikipedia.org/wiki/Information_security
2. https://sites.google.com/site/uisgua
3. https://www.issa.org
4. https://www.president.gov.ua
5. https://www.rada.gov.ua

ДОДАТОК А

Титульна сторінка розрахунково-графічної роботи

Міністерство освіти і науки України

Чернігівський національний технологічний університет

Навчально-науковий інститут управління та адміністрування

Факультет життєдіяльності, природокористування та туризму

Кафедра кібербезпеки та математичного моделювання

КОНТРОЛЬНА РОБОТА

з дисципліни « Інформаційна безпека держави »

на тему «_____»

студента (тки) групи _____

П.І.П. _____

варіант _____

Перевірив:

_____

_____

_____

(П.І.П., посада)

Чернігів 2017 р.

ДОДАТОК Б

Приклади оформлення літературних джерел

Державні стандарти:

1. Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (macs). Частина 3. Механізми, що використовують універсальну геш-функцію. ДСТУ ISO/IEC 9797-3:2015 (ISO/IEC 9797-3:2011, IDT) – [Чинний від 2017-01-01]. – К.: Держстандарт України, 2017. – 50 с. – (Державний стандарт України).
2. Інформаційні технології. Основні напрямки оцінювання та відбору CASE-інструментів (ISO/IEC 14102:1995) – ДСТУ 3919-1999 [Чинний від 2000-01-01]. – К.: Держстандарт України, 2000. – 470 с. – (Національний стандарт України).

Книги:

3. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / МВС України, Ун-т внут. справ - Х., 2010. -366с.
4. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,;// Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005. - 432 с.
5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
6. Володимир Горобцов, Андрій Колодюк, Борис Кормич: Правове забезпечення інформаційної діяльності в Україні / Володимир Горобцов, Андрій Колодюк, Борис Кормич та ін.; Ред. І. С. Чиж;// Ін-т держави і права ім. В.М.Корецького, Нац. Академія Наук України, Держ. комітет телебачення і радіомовлення України. -К.: Юридична думка, 2006. -384 с.
7. Глобалізація і безпека розвитку / [Білорус О. Г., Гончаренко М. О., Зленко В. А. та ін.]; НАН України, Київ. нац. екон. ун-т. - К.: КНЕУ, 2011. - 733 с.
8. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Ірина Маракова, Анатолій Рибак, Юрій Ямпольский;// Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій. - Одеса, 2001. -164 с.
9. Ліпкан В.А. Управління системою національної безпеки України. — К.: КНТ, 2006. — 68 с (Серія: Національна і міжнародна безпека).

Статті:

10. Актуальні проблеми інформаційної безпеки України. Аналітична доповідь УЦЕПД / /Національна безпека і оборона. - К.: 2001. -№1. - С.2-59.
11. Гуцалюк М. Інформаційна безпека України: нові загрози / Гуцалюк М. // Бизнес и безопасность. - 2003. - № 5. - С. 2-3.
12. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ // Актуальні проблеми економіки. - 2006. - № 10. - С. 220 - 225.
13. Куберт П. Обеспечение безопасности при эксплуатации по ISO 17799 // Бизнес и безопасность. - 2007. - № 1(57).

Електроні ресурси:

14. ISO/IEC 17799 2005 Information Security Management Standard[Електронний ресурс]//Режим доступу - http://www.jetinfo.ru/2004/11/3/article3.11.2004.html
15. Стандарт ISO 15408: 1999-1-3 Методы и средства обеспечения безопасности. [Електронний ресурс] // Режим доступу - http://www.jetinfo.ru/2004/11/3/article3.11.2004.html
16. Закон України «Про стандартизацію» від 17.05.2001 р. [Електронний ресурс]// Режим доступу- www.rada.gov.ua.
17. Федеральный стандарт США FIPS 140-2 [Електронний ресурс] // Режим доступу - http://www.jetinfo.ru/2004/11/3/article3.11.2004.html

18. О.М. Богданов, О.О. Бакалинський «Адаптація міжнародного стандарту управління інформаційною безпекою ISO/IEC 27001:2005 у структурах державного управління України» [Електронний ресурс]// Режим доступу до статті: - http://nc.nusta.com.ua/Kyrsi%202009/tezi/images_tezi/S_6_Bogdan v_Bakalynsky_1.htm