ПРОГРАМА

фахового іспиту при вступі на навчання
для здобуття ступеня магістра за спеціальністю
125 Кібербезпека та захист інформації
(освітньо-професійна програма «Управління інформаційною безпекою»)

1. Мета тестування

Тестування проводиться з метою:

- перевірки відповідності знань, умінь та навичок курсантів, студентів та слухачів (надалі слухачів) програмовим вимогам;
- виявлення та оцінки рівня навчальних досягнень слухачів;
- оцінки ступеня підготовленості вступників до навчання за спеціальністю 125 Кібербезпека та захист інформації (освітньо-професійна програма: Управління інформаційною безпекою) для здобуття ступеня магістра.

Зміст тестових завдань визначається фаховою атестаційною комісією відповідно до змісту освіти та державних вимог до рівня підготовки вступників.

Завдання вступного випробування полягає у тому, щоб оцінити в слухачів загально-професійні та спеціалізовано-професійні компетенції.

2. Загально-професійні компетенції:

- базові уявлення про поняття інформації та інформаційних відносин, систему й рівні інформаційного забезпечення управлінської діяльності;
- базові знання про складові та функціональні процеси системи інформаційної безпеки й уміння їх використовувати в професійній діяльності;
- сучасні знання про протидію загрозам інформаційному суверенітету держави й уміння їх використовувати;
- здатність аналізувати основні проблеми інформаційної сфери, організовувати власну діяльність з огляду на досягнення науки управління та з урахуванням динамічних змін, що відбуваються у сфері інформаційної безпеки;
- сучасні уявлення про розробку проектів нормативно-правових актів, які спрямовані на забезпечення інформаційної безпеки держави на засадах конституційно-правової регламентації законодавчого й нормотворчого процесів;
- здатність вирішувати окремі завдання забезпечення системи інформаційної безпеки на всіх циклах її існування;
- базові уявлення про різні моделі управління та методи оцінювання суспільно-політичної й економічної ситуації з огляду на трансформаційні процеси розбудови держави та необхідність розв'язання проблем забезпечення інформаційної безпеки;
- уявлення про напрями державної інформаційної політики;
- базові уявлення про деструктивні інформаційно-психологічні впливи та операції;
- базові уявлення про новітні інформаційні технології;
- базові уявлення про створення організованої, повноцінної, ефективної, дієвої системи управління інформаційною безпекою на підприємстві, в установі, органі державного управління;
- уявлення про сучасні дійові загальнодержавні інформаційні системи насамперед у соціальних сферах охорони здоров'я, освіти, науки, культури, охорони довкілля;
- знання, удосконалення й застосування на практиці організаційної структури системи управління інформаційною безпекою;
- сучасні уявлення про принципи моніторингу, оцінювання стану інформаційної інфраструктури та інформаційного простору держави;

- здатність планувати, приймати й реалізовувати заходи у сфері управління інформаційною безпекою;
- знання правових основ дослідних робіт і законодавства України в інформаційній сфері;
- здатність організувати роботу відповідно до вимог безпеки життєдіяльності й охорони праці;
- здатність до ділових комунікацій у сфері інформаційної безпеки, знання основ ділового спілкування, навички роботи в команді;
- уміння вести дискусію й навчати співробітників новим методам забезпечення інформаційної безпеки держави;
- здатність використовувати наукову організацію управлінської праці співробітників, задіяних у системі забезпечення інформаційної безпеки;
- знання про інформацію з обмеженим доступом для забезпечення її базових характеристик безпеки (конфіденційність, цілісність, доступність);

3. Спеціалізовано-професійні компетенції:

- здатність використовувати професійно профільовані знання в галузі математики (математичної статистики) для статистичного оброблення експериментальних даних і математичного моделювання інформаційної безпеки держави;
- здатність використовувати математичний апарат для засвоєння теоретичних основ і практичного використання сучасних методів дослідження інформаційної безпеки;
- здатність використовувати професійно профільовані знання й практичні навички для прогнозування рівня небезпечності інформаційного розвитку суспільства та його складових на середньострокову й довгострокову перспективу на основі оцінки існуючого стану справ з урахуванням наявних тенденцій та впливу комплексу внутрішніх і зовнішніх чинників на реалізацію національних інтересів в інформаційній сфері;
- здатність використовувати теоретичні знання й практичні навички для оволодіння основами теорії й методів досліджень у галузі інформаційної безпеки;
- здатність використовувати професійно профільовані знання і практичні навички для організації забезпечення обладнання підрозділів інформаційної безпеки необхідними організаційними та технічними засобами;
- здатність використовувати знання, уміння й навички з метою розроблення системи управління інформаційною безпекою;
- здатність використовувати професійно профільовані знання в галузі інформаційної безпеки для проектування загроз інформаційній безпеці;
- здатність використовувати знання й уміння для прогнозування, виявлення та оцінювання можливих загроз інформаційному простору держави, дестабілізуючих чинників;
- здатність використовувати професійно профільовані знання, уміння й навички для формування системи (органів, підрозділів), що забезпечують інформаційну безпеку;
- здатність використовувати знання, уміння й навички в галузі інформаційної безпеки для теоретичного засвоєння загально-професійних дисциплін і вирішення практичних завдань;
- професійно профільовані знання й уміння в галузі теоретичних основ інформатики й практичного використання комп'ютерних технологій;
- володіння навичками роботи з комп'ютером на рівні користувача, здатність використовувати інформаційні технології для вирішення експериментальних і практичних завдань у галузі професійної діяльності;

- здатність використовувати професійно профільовані знання й практичні навички для розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами;
- здатність використовувати теоретичні знання й практичні навички для розробления, організації розроблення та здійснення побудови системи організаційно-службових і спеціальних заходів із забезпечення інформаційної безпеки установ, підприємств, організацій;
- здатність використовувати професійно профільовані знання й практичні навички для забезпечення результативної та ефективної взаємодії державних установ і організацій зі спеціальними та правоохоронними органами у сфері управління й забезпечення інформаційної безпеки;
- здатність використовувати професійно профільовані знання, уміння й навички щодо аналізу розвитку сучасних технологій вітчизняної та зарубіжної індустрії інформації.

4. Зміст програми

Назва дисципліни та блоку змістових модулів	Назва змістового модуля
1	2
Інформаційна безпека держави	
Сутність небезпек інформаційній безпеці. Основи забезпечення інформаційної безпеки держави	Поняття інформаційної безпеки держави, суспільства та особи. Небезпеки для інформаційної безпеки держави, особи та суспільства. Обмеження свободи слова і доступу громадян до інформації. Негативні чинники впливу на інформаційну безпеку у сфері суспільної моралі. Правопорушення у сфері інформаційних технологій. Правові засади забезпечення інформаційної безпеки держави. Основи державної політики у сфері забезпечення інформаційної безпеки держави. Інститути громадянського суспільства як суб'єкти забезпечення інформаційної безпеки. Юридична відповідальність за правопорушення у сфері забезпечення інформаційної безпеки держави.
Безпека життєдіяльності (основи екології, екологія інформаційних технологій, основи охорони праці, цивільна оборона)	
Фактори середовища мешкання людини, причини та джерела руйнування біосфери, засоби радіаційної, хімічної розвідки й дозиметричного контролю, засоби та основні способи захисту населення й територій при виникненні надзвичайних ситуацій природного, техногенного, соціально-політичного та воєнного характеру	Основні поняття екології. Глобальні проблеми екології. Природоохоронне законодавство в Україні. Законодавча й нормативна база щодо безпеки життя та діяльності людини в Україні, основні положення загальної безпеки. Загальні правила безпеки людини в побутових умовах та спеціальні правила безпеки на підприємстві. Основні характеристики середовища мешкання людини. Характеристика шкідливих та небезпечних факторів, які можуть виникнути при аваріях, катастрофах та стихійних лихах, і заходи щодо захисту від них. Основи організації захисту об'єктів підприємства та співробітників при загрозі й виникненні надзвичайних ситуацій. Загальні положення про організацію ліквідації наслідків аварій, катастроф та стихійних лих. Засоби і заходи долікарської допомо-

1	2
	ги при ураженнях РНР, ХНР та БНР. Основні принципи планування захисних заходів щодо попередження надзвичайних подій та ліквідації їх наслідків, здійснення евакозаходів. Організація роботи штабів із надзвичайних ситуацій, оперативно-слідчих груп.
Алгоритмічні основи криптології	
Теоретичні та практичні аспекти побудови та застосування методів криптографічного захисту інформації в системах спеціального зв'язку, електронного документообігу та електронної комерції. Нормативно-правове регулювання діяльності у галузі криптографічного захисту інформації.	Основні положення криптографічного захисту інформації (далі – КЗІ). Класифікація методів КЗІ, історичні етапи розвитку. Методи симетричної криптографії. Математичні моделі симетричних шифрів та їх основні властивості. Методи асиметричної криптографії. Математичні задачі асиметричної криптографії та їх основні характеристики. Криптографічні протоколи. Методи їх побудови та оцінювання криптографічної стійкості. Нормативно-правове регулювання у галузі КЗІ. Основні напрямки розвитку сучасної криптографії. Стан та напрямки розвитку сучасних систем КЗІ.
Основи технічного захисту інформації	
Теоретичні та практичні аспекти перекриття можливих технічних каналів витоку інформації та несанкціонованого доступу до неї, ознайомлення з класифікацією і структурою технічних каналів витоку інформації, принципами дії технічних засобів розвідки, завданнями ТЗІ, структурою та функціонуванням системи ТЗІ в Україні.	Класифікація і структура технічних каналів витоку інформації. Принципи дії технічних засобів розвідки. Завдання технічного захисту інформації. Структура та функціонування системи ТЗІ в Україні. Теоретичні та практичні аспекти перекриття можливих технічних каналів витоку інформації та несанкціонованого доступу до інформації.
Теорія ризиків	
Природа та основні види ризику у сфері інформаційної безпеки. Види аналізу ризиків проектів.	Природа й основні види ризику у сфері інформаційної безпеки. Шляхи зменшення ризиків у сфері інформаційної безпеки. Шляхи попередження та подолання кризових ситуацій у сфері інформаційної безпеки. Види аналізу ризиків проектів. Основні перспективні напрями розвитку інформаційних технологій захисту інформації. Оцінка ризиків. Технічні, прикладні, системні програмні засоби підтримання та захисту інформації.
Організаційне забезпечення захисту інформації	
Організаційно-правові основи захисту інформації з обмеженим доступом та особливості захисту певних видів інформації.	Правовий статус інформації. Поняття інформації як виду власності. Класифікація інформації. Поняття й зміст інформації з обмеженим доступом. Поняття та система захисту інформації з обмеженим доступом. Поняття охорони державної таємниці. Правові основи захисту комерційної таємниці. Міжнародно-правові основи захисту інформації з обмеженим до-

1	2
	ступом. Правовий статус та зміст інформації з обмеженим доступом про особу.
Спеціальне діловодство	
Загальні та практичні знання з основ секретного й конфіденційного діловодства.	Діловодство. Правові основи діловодства. Види діловодства. Особливості ведення секретного діловодства. Особливості ведення конфіденційного діловодства. Значення секретного та конфіденційного діловодства для належного функціонування підприємств, установ, організацій. Значення секретного й конфіденційного діловодства для судового розгляду спорів різного виду.
Управління персоналом	
Знання, необхідні для ефективного управління персоналом, навички створювати умови для роботи, за яких працівники можуть задовольнити свої потреби, забезпечуючи водночас досягнення цілей підприємством.	Поняття і принципи управління персоналом на підприємствах різного профілю й форм власності. Законодавчі та нормативні акти, що регулюють управління персоналом і регламентують трудові правовідносини. Структура персоналу, мета призначення і структура системи керування персоналом. Кадрове, інформаційне й технічне забезпечення системи. Прогнозування та планування роботи з персоналом. Сучасні принципи і методи підбору й розстановки кадрів. Аналіз професійних і особистісних якостей претендентів на одержання роботи чи призначення на посаду. Методики тестування, анкетування і ведення співбесід. Критерії ухвалення рішення про прийом на роботу. Організація роботи з персоналом. Порядок роботи, методи інструктування і навчання співробітників. Контроль якості й кількості праці кожного співробітника, оціночні показники. Моральне і матеріальне стимулювання праці, висування по службі. Критерії накладання дисциплінарних стягнень.
Безпека інформації в інформаційно-телекомунікаційних системах	
Проблема уразливості інформації в сучасних КС оброблення даних, чинне нормативно-правове забезпечення в цій галузі, вивчення методології захисту інформації в КС інформаційними технологіями захисту та захищеними технологіями оброблення, безпосереднє практичне використання отриманих відомостей для організації захисту інформації на об'єктах інформаційної діяльності.	Основні загрози інформації в КС. Апаратно-програмні методи та заходи захисту інформації в КС. Організаційно-режимні аспекти захисту інформації в КС. Структура й обов'язки підрозділу технічного захисту інформації в КС.
Прогнозування та моделювання в соціальній сфері	
Основи сучасного системного	Термінологія та зміст основних понять системного аналізу, про-

1	2
аналізу та його застосування в менеджменті проектів, системах захисту інформації, ключові поняття та методи математичного моделювання. Класифікація моделей, застосування моделей для прогнозу стану соціальної сфери, імітаційне моделювання складних систем, структуризація та формалізація опису соціаль-них систем за результатами системного аналізу.	гнозування та моделювання. Методи декомпозиції й структуризації складних систем. Методи структурної ідентифікації об'єктів і процесів. Моделювання. Моделі. Класифікація, методи параметричної ідентифікації моделей. Прогнозування. Методи прогнозування. Моделювання і прогнозування в соціальній сфері.
Менеджмент інформаційної безпеки	
Система нормативно-правового регулювання суспільних відносин в інформаційній сфері, вивчення основних законодавчих актів України, формування у студентів достатнього рівня знань для управління і правильного застосування чинного законодавства на практиці.	Система законодавства у сфері інформаційних відносин. Загальні принципи внутрішньої й зовнішньої політики держави у сфері інформаційних відносин. Об'єкти та суб'єкти інформаційних відносин, основні права й обов'язки учасників зазначених відносин. Види інформації, загальні принципи охорони інформації з обмеженим доступом. Законодавче забезпечення права власності (у тому числі інтелектуальної) на інформацію. Відповідальність за порушення законодавства у сфері інформаційних відносин.
Система охорони державної таємниці	
Принципи, заходи, засоби й умови організаційного захисту інформації; порядок засекречування й розсекречення відомостей, документів і продукції; допуск і доступ до конфіденційної інформації й документів.	Організація внутрішньо-об'єктового й пропускного режимів на підприємствах. Організація підготовки та проведення нарад і засідань із конфіденційних питань. Організація охорони підприємств. Захист інформації при рекламній діяльності. Організація аналітичної роботи з попередження витоку конфіденційної інформації. Напрями й методи роботи з персоналом, котрий володіє конфіденційною інформацією.
Інформаційне забезпечення управлінської діяльності	
Теоретичні та практичні аспекти інформаційного забезпечення управлінської діяльності різних рівнів, з сучасними інформаційними технологіями, плануванням та оптимізацією дій на стадії збирання, аналізу та оброблення інформації, прийняття рішення, контролю його виконання.	Теоретичні засади та принципи створення інформаційних систем. Головні компоненти інформаційного, технічного, програмного й організаційного забезпечення, використовуваного в управлінських інформаційних системах. Сучасні комп'ютерні інформаційні технології, що базуються на застосуванні новітніх розробок у галузі штучного інтелекту, зокрема експертні системи, бази знань, системи підтримки прийняття рішень. Сучасні телекомунікаційні технології забезпечення управлінської діяльності, електронний документообіг, електронний цифровий підпис.
Технології програмування	
Теоретичні та практичні аспе-	Мови програмування низького рівня.

1	2
кти автоматизації оброблення даних шляхом реалізації алгоритму оброблення у вигляді впорядкованої послідовності інструкцій для обчислювальної машини, спеціальні системи запису цих інструкцій, уніфіковані нормальні засоби фіксації програм – мови програмування.	Мови програмування високого рівня. Мови програмування в базах даних. Об'єктно-орієнтовані мови програмування.
Комплексні системи захисту інформації	
Сутність методів та засобів комплексної системи захисту інформації (КСЗІ). Принципи організації й етапи розроблення КСЗІ. Фактори, що впливають на організацію КСЗІ. Визначення й нормативне закріплення складу захисту інформації, щодо визначення об'єктів захисту. Аналіз й оцінювання загроз безпеці інформації. Нормативно-правові аспекти створення КСЗІ.	Основні положення, Загальна класифікація загроз. Об'єкт, предмет, мета та завдання комплексного захисту інформації. Визначення й завдання комплексу технічного захисту інформації. Технічні канали витоку інформації. Фізика технічних каналів витоку мовної та візуальної інформації на ОІД. Класифікація методів і засобів прослуховування, спостереження і знімання інформації на ОІД. Матеріально-речові канали витоку інформації на ОІД. Технічні канали витоку, нав'язування, знищення та блокування інформації в ІТС. Методи й засоби захисту інформації на ОІД. Архітектурно-будівельні заходи, методи та засоби пасивного й активного захисту ОІД, методи та засоби виявлення й нейтралізації засобів несанкціонованого доступу. Методи та засоби захисту інформації в ІТС. Методи та засоби інженерно-технічних заходів безпеки. Нормативно-правове регулювання у сфері ТЗІ та КЗІ. Порядок проведення робіт із створення комплексу ТЗІ. Порядок проведення робіт із створення КСЗІ.

5. Література

1. Акт проголошення незалежності України // Відомості Верховної Ради України, 1991. – № 38. – Ст. 502.
2. Антонюк А.О. Основи захисту інформації в автоматизованих системах : навч. посібн. – НУ "Києво-Могилянська академія", 2003 – 244 с.
3. Бабак В.П., Корченко О.Г. Інформаційна безпека та сучасні мережеві технології. Англо-українсько-російський словник термінів, Київ: НАУ, 2003. – 670 с.
4. Борзов Ю.О., Малець І.О., Рак Т.Є. Провідні засоби зв’язку підрозділів МНС. – Львів : Вид-во НУ "Львівська політехніка", 2007. – 108 с.
5. Браіловський М.М., Лазарєв Г.П., Хорошко В.О. Захист інформації в банківській діяльності. – Вид. 2-ге, [перероб. та доп.]. – К. : ТОВ “Поліграф-Консалтінг", 2004. – 216 с.
6. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок. – К.: НАУ, 2013. – 432 с.
7. Бутузов В. М. Протидія комп’ютерній злочинності в Україні (системно структурний аналіз): монографія / В. М. Бутузов. – К.: КІТ, 2010. – 145 с.
8. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации. – Владивосток: Изд-во ДВГТУ, 2007. – 318 с.
9. Василюк В.Я., Климчук С.О. Інформаційна безпека держави: курс лекцій. К. : КНТ. Видавничий дім “Скіф", 2008. – 136 с.

10. Витяг з Кримінально-процесуального кодексу України (зі змінами і доповненнями) від 28 грудня 1960 року : підручник / М.І. Камлик. Судова бухгалтерія. – Вид. 4-те, [перероб. та доп.]. – К. : Вид-во "Атіка", 2003. – С. 398.
11. Гарасимчук О.І., Дудикевич В.Б., Ромака В.А. Комплексні системи санкціонованого доступу : навч. посіб. Нац. ун-т "Львів. політехніка". – Львів. : Вид-во Львів. політехніки, 2010. – 212 с.
12. Гончаров С.М. Основи економічної безпеки підприємства : навч. посібн. / Гончаров С.М., Кузнєцова Т.В., Лесняк О.Ю. – К. : Кондор-Видавництво, 2012. – 216 с.
13. Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах : навч. посібн. Ч.1. Криптографічний захист інформації – Харків : Вид-во ХНУРЕ, 2004. – 368 с.
14. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К. : Видавнича група BHV, 2009. – 608 с.
15. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія / Р. В. Грищук. – Житомир: Рута, 2010. – 280 с.
16. ДБН А.2.2. – 2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва, затверджений наказом Держкоммістобудування України № 156 від 02.09. 96 р. Чинний від 01.01.97 р.
17. Домарев В.В. Безопасность информационных технологий: Системный подход. – К. : ООО "ТИД ДС", 2004. – 992с.
18. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності : навч. посібн. для ВНЗ. – К. : Вид-во ЄУФІМБ, 2006. – 102 с.
19. Донець Л.І. Економічна безпека підприємства : навч. посібн. / Л.І. Донець, Н.В. Ващенко. – К. : Центр навч. літ-ри, 2008. – 240 с.
20. Дубов, Д. В. Кібербезпека: світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К.: НІСД, 2011. – 30 с.
21. Дудикевич В.Б., Хома В.В., Пархуць Л.Т. Захист засобів і каналів телефонного зв'язку : навч. посібн. – Львів : Вид-во Львівської політехніки, 2012. – 212 с.
22. Економічна безпека : навч. посіб. / О.Є. Користін, О.І. Барановський, Л.В. Герасименко та ін. К. : Алерта; КНТ. Центр навч. літ-ри, 2010. – 368 с.
23. Економічна безпека підприємств : підручник / Ортинський В.Л., Керницький І.С., Живко З.Б. та ін. – К. : Алерта, 2011. – 704 с.
24. Економічна безпека підприємств, організацій та установ : навч. посібн. / В.Л. Ортинський, І.С. Керницький, З.Б. Живко та ін. К. : Правова єдність, 2009. – 544 с.
25. Захист економічної інформації : уавч. посібн. / [Браіловський М.М., Дорошко В.О., Чирков Д.В., Шелест М.Е.]; ра ред. проф. В.О. Хорошка. – К. : НАУ, 2002. – 78 с.
26. Зубок М.І. Безпека банківської діяльності : навч. посібн. / Зубок М.І. – К. : КНЕУ, 2002. – 190 с.
27. Іванюта Т.М. Економічна безпека підприємства навч. посібн. [для студ. вищ. навч. закл.] / Т.М. Іванюта, А.О. Заїчковський. – К. : Центр навч. літ-ри, 2009. – 256 с.
28. Калмик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посібн. / М.І. Калмик. – К. : Вид-во "Атіка", 2005. – 432 с.
29. Колот А. М. Мотивація, стимулювання й оцінка персоналу. – К., 1998.
30. Корченко О. Г. Класифікація методів соціального інжинірингу / О. Г. Корченко, Є. В. Паціра, Д. А. Пуха // Захист інформації. – К.: НАУ. – 2007. – № 4. – С. 37–45.
31. Кримінальний кодекс України. Прийнятий сьомою сесією Верховної Ради України 5 квітня 2001 р. – Київ: Юрінком-Інтер, 2001.
32. Крушельницька О.В., Мельничук Д.П. Управління персоналом. – Київ, 2006р.
33. Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Issue. 2 (13). P. 126–136.

34. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах / под ред. В.А. Хорошко. – К. : Арий, 2008. – Том 1. Несанкционированное получение информации. – 464 с.
35. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах / под ред. В.А. Хорошко. – К. : Арий, 2008. – Том 2. Информационная безопасность. – 344 с.
36. Мурашко М.І. Менеджмент персоналу. – К.: «Знання», 2002.
37. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – Київ: ТОВ "Поліграф консалтинг", 2005. – 240 с.
38. Павленко Н. Трудові відносини: запитання та відповіді. – Х.: «Фактор», 2001. Пасічник В. В., Резніченко В. А. Організація баз даних і знань. – BHV, Киев, 2006. – 384 с.
39. Петюх В.М. Управління персоналом: Навч.-метод. посібник для самостійного вивчення дисципліни. - К., 2000.
40. Положення про технічний захист інформації в Україні, затверджене постановою Кабінету Міністрів України від 9 вересня 1994 р., № 632 // ЗП України. – 1994. – № 12.
41. Положення про технічний захист інформації в Україні: Закон України від 02.06.2000 № 1775-Ш // Відомості Верховної Ради України. – 2000. – № 36. – Ст. 299.
42. Про захист інформації в автоматизованих системах : Закон України // Відомості Верховної Ради. 1994. – №31. – 286 с.
43. Про інформацію : Закон України від 2 жовтня 1992 р., № 2657-XII.
44. Про наукову і науково-технічну діяльність [Електронний ресурс]. – Електрон. дан. – К. : Верховна Рада України. – Режим доступу: http: // zakon1. rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1977-12, вільний. Назва з екрану.
45. Про основи національної безпеки України: Закон України від 19 червня 2003 р // Офіц. Вісн. України. – 2003. – № 29. – Ст. 1433.
46. Про розвідувальні органи : Закон України від 22 березня 2001 р., № 2331-Ш // Відомості Верховної Ради України.
47. Рамський Ю.С., Олексюк В.П., Балик А.В. Адміністрування комп'ютерних мереж і систем: Навч. пос. – Тернопіль: Навчальна книга – Богдан, 2010. – 196 с.
48. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О.. Організаційно-технічне забезпечення захисту інформації. К. : НАУ, 2002. – 207 с.
49. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша – К.: ВБ «Аванпост-Прим», 2012. – 214 с.
50. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К. : Юниор, 2003. – 504с.
51. Цивільний кодекс України від 16 січня 2003 р., № 435-IV. – Нове законодавство України / Уклад. Ю.П. Єлісовенко. – К. : Вид-во "Махаон", 2003. – 600 с.