СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Інформаційно-психологічне протиборство
Мова викладання	українська
Викладач (-і)	Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, д.пед.н., доцент
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ ORCID 0000-0002-8565-0525
Контакти викладача	(063) 594 22 94 tkachym79@gmail.com

1. Анотація курсу -

Предметом навчальної дисципліни "Інформаційно-психологічне протиборство" (ІПсП) є сутність, зміст та історія ІПсП.

Об'єкт навчальної дисципліни - інформаційно-психологічна складова національної безпеки.

Організаційні форми, методи й засоби забезпечення високої фундаментальної, професійної і практичної спрямованості та диференційованого підходу навчання студентів: для ефективної організації навчальних занять використовуються такі форми роботи, як розповідь, навчальна лекція, лабораторна робота, дискусія, робота з книгою та в Інтернеті, постановки завдання, планування процесом виконання, ілюстрування, демонстрування, регулювання й контроль, аналіз підсумків лабораторної роботи.

Практична та професійна спрямованість дисципліни зумовлена набуттям знань і вмінь щодо управління інформаційною безпекою. Насамперед, це знання та вміння, які дають змогу виявляти загрози національній безпеці в інформаційній сфері, аналізувати сучасний стан системи забезпечення інформаційної безпеки України й розробляти пропозиції щодо її вдосконалення.

МОДУЛЬ 1.
СУТНІСТЬ ТА ЗМІСТ ІНФОРМАЦІЙІЮ-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

ТЕМА 1. Сутність інформаційної безпеки

Інформація, принципи, суб'єкти, об'єкти інформаційних відносин. Інформаційна діяльність, інформаційні ресурси. Інформаційний суверенітет і шляхи його забезпечення. Інформаційна безпека та її різновиди. Інформаційно-технічні впливи й безпека інформаційно-технічної інфраструктури. Переконання та навіювання як базові методи інформаційно-психологічного впливу (ІПсП). Сутність маніпулювання. Базові методи ІПсП. Алгоритми здійснення переконання та навіювання. Умови, від яких залежить ефективність проведення ІПсП. Джерела загроз інформаційно-психологічній безпеці людини в міжособистісній комунікації. Перекручування, приховування та спосіб

подання інформації як методи маніпулювання. Засоби примушування, які використовуються в маніпулятивному впливі. Роботизація і зміни в індивідуальній свідомості, які може спричинити ІПсП. Організаційні ознаки виявлення маніпулювання через ЗМІ. Змістовні ознаки виявлення маніпулювання через ЗМІ.

ТЕМА 2. Зміст інформаційно-психологічного протиборства

Форми і види інформаційного протиборства. Об'єкти посягань та завдання інформаційної війни. Об'єкти деструктивного інформаційного впливу й форми інформаційної війни. Характеристика основних видів інформаційної зброї. Етапи, ознаки та суб'єкти проведення спеціальних інформаційних операцій. Методи спеціальних інформаційних операцій: дезінформування, пропаганда, диверсифікація громадської думки, психологічний тиск і поширення чуток. Чинники ескалації загроз і небезпек в інформаційно-ідеологічній сфері: їхні джерела та сутність. Основні загрози національній безпеці в інформаційній сфері. Заходи, які необхідно вживати для забезпечення інформаційної безпеки України.

МОДУЛЬ 2. ІСТОРІЯ ТА СУЧАСНИЙ СТАН ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

ТЕМА 1. Становлення і розвиток ІПсП

Китайські стратегеми і положення про ІПсП "Трактату про військове мистецтво" Сунь-Цзи. Спеціальна пропаганда давніх Греції та Риму. ІПсП епохи середньовіччя. Зародження пропаганди як форми інформаційно-психологічного впливу в епоху Середньовіччя. Особливості ІПсП за часів українського козацтва. Форми інформаційно-психологічного впливу, які використовував Наполеон після приходу до влади. Особливості ІПсП у підготовці та проведенні війні Б.Наполеона в Росії 1812 року. Особливості проведення спецпропаганди військами О.Суворова та М.Кутузова.

ТЕМА 2. Формування основ теорії і практики ІПсП в роки Першої світової війни та в міжвоєнний період

Особливості спецпропаганди у роки Першої світової війни. Політичний досвід використання пропаганди у Першій світовій війні. Більшовицька пропаганда - основа діяльності політорганів Червоної армії серед військ противника. Радянська пропаганда серед військ і населення противника у роки громадянської війни й іноземної інтервенції. Особливості здійснення пропагандистського впливу на противника перед Фінською війною. Зародження нацистської пропаганди в Німеччині та прихід А.Гітлера до влади. Заснування організації "СС-Аненербе" та її функції у фашистській Німеччині. Основні напрямки діяльності нацистської пропаганди.

ТЕМА 3. ІПсП в роки Другої світової війни

Роль воєнної пропаганди Німеччини у збройних конфліктах. Особливості здійснення інформаційно-психологічного впливу фашистською Німеччиною на території України. Заходи радянського уряду напередодні Другої світової війни для зміцнення апарату спецпропаганди. Особливості та напрями ведення спецпропаганди СРСР у роки Другої світової війни. Особливості пропаганди США на війська та населення противника. Організація та проведення

пропаганди на війська і населення противника урядом Англії. Організація та здійснення інформаційно-психологічного впливу Японією в роки Другої світової війни.

ТЕМА 4. ІПсП часів "холодної війни"

Нові концепції та погляди США на ведення психологічної війни у Кореї (1950-1953 рр.). Випробування концепції спеціальних методів війни США під час війни у В'єтнамі (1964-1975). Особливості психологічної операції під час агресії США проти Гренади 1983 року. Психологічна операція під час вторгнення ЗС США у Панаму - подальший розвиток теорії локальних війн (грудень 1989 - січень 1990). Особливості психологічних операцій ЗС США у Перській затоці (1991). Аналіз внутрішніх політичних та економічних причин розвалу СРСР. Недооцінка військово-політичним керівництвом СРСР ролі та значення інформаційних факторів "холодної війни". Керівні документи США, направлені на здійснення постійного інтенсивного інформаційного впливу на СРСР.

ТЕМА 5. Особливості сучасного стану ІПсП

Основні тенденції зміни характеру геополітичної боротьби держав та розвиток процесу глобалізації сучасності. Інформаційно-психологічні операції, як альтернатива бойовим діям. Лінійний та синергетичний підходи до спеціальних інформаційних операцій. Інформаційний простір - театр сучасних військових дій. Класифікація сучасної інформаційної зброї. Основні способи і методи застосування інформаційної зброї. Міжнародний "кібертероризм", інформаційні та інформаційно-іміджеві війни сучасності. Нові форми і методи інформаційного впливу на психіку людини. Індивідуальна, групова і масова свідомість людей - основні об'єкти агресивного ІПсВ.

ТЕМА 6. ІПсП крізь призму засобів масової комунікації

Взаємозалежність та взаємозумовленість ІПсП й модифікацій засобів масової комунікації (ЗМК). Сутність переваг та проблем, що виникають при веденні ІПП за допомогою ЗМК. Характеристика ІПсП, що здійснюється за допомогою ЗМК. Етапи становлення ЗМК. Тренди у сфері комунікацій, які впливають на участь сучасних ЗМК в ІПсП. Техніки маніпуляції, що застосовуються ЗМК при здійсненні інформаційно-психологічних впливів. Характеристика військових ЗМК

2. Мета та цілі курсу -

Метою викладання дисципліни є надання випускникам системних знань, умінь і навичок для подальшого використання у своїй практичній діяльності по захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів з урахуванням досягнень науково-технічного прогресу та міжнародного досвіду.

Завдання полягає у:

- отриманні знань про понятійний апарат з інформаційної безпеки держави; загрози національній безпеці; еволюцію інформаційно-психологічного протиборства; сучасні технології та акції проведення акцій інформаційного впливу; спеціальних інформаційних операцій, інформаційних війн;

- набутті умінь з узагальнення теоретичних уявлень щодо сутності інформаційної безпеки, виявлення наявних та потенційних загроз національній безпеці України в інформаційній сфері, прихованих і шкідливих інформаційно-психологічних впливів, формування критичного мислення; прогнозування можливих небезпек стосовно інформаційного простору держави.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

3. Результати навчання –

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 2. планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 4. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 5. реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

У результаті вивчення навчальної дисципліни студент повинен:

Знати:

— базові поняття щодо інформаційної безпеки держави, суспільства і особи;
— види та сучасні технології інформаційних впливів;
— сутність форми і види інформаційного протиборства;
— етапи, ознаки, суб'єкти та методи проведення спеціальних інформаційних операцій;
— завдання, об'єкти посягань, форми проведення інформаційної війни;
— історію і особливості сучасного стану інформаційно-психологічного протиборства;

— основні методи, головні вектори та види атак з використанням соціальної інженерії.

Вміти:

— узагальнювати теоретичні уявлення щодо сутності інформаційної безпеки;
— виявляти існуючі та потенційні загрози національній безпеці України в інформаційній сфері;
— виявляти приховані та шкідливі інформаційно-психологічні впливи;
— здійснювати порівняльний аналіз форм, методів, засобів та технологій проведення інформаційних війн, акцій інформаційного впливу та спеціальних інформаційних операцій;
— здійснювати прогнози щодо можливих небезпек інформаційному простору держави;
— використовувати світовий досвід щодо захисту інформаційного простору для його творчого впровадження на українських теренах.

4. Обсяг курсу. Зазначте загальку кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	**Загальна к-сть годин**
лекції	16
лабораторні	14
самостійна робота (РГР)	60

5. Пререквізити - Взаємозв'язок із суміжними дисциплінами: вивчення навчальної дисципліни "Інформаційно-психологічне протиборство" поглиблює знання студентів отримані під час вивчення таких дисциплін "Історія України", "Інформаційна безпека держави", "Забезпечення інформаційної безпеки" й "Основи національної безпеки" (при підготовці фахівців освітньо-кваліфікаційного рівня "бакалавр" за напрямом "Кібербезпека)". Дисципліна "Соціальна інженерія" дає фундаментальні знання для вивчення пропонованої дисципліни.

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

• практичні роботи : 20% семестрової оцінки;
• домашні завдання: 20% семестрової оцінки;
•РГР: 20% семестрової оцінки;
• іспит: 40% семестрової оцінки.

Загальна система оцінювання курсу	Інформаційно-психологічне протиборство
Вимоги до РГР	**Критерії оцінювання написання** 1. Повнота розкриття. 2. Авторський внесок. 3. Актуальність.

	4. Практична значимість. 5. Відповідність вимогам оформлення. **Вимоги оформлення** Об'єм 15-25 сторінок. 14 шрифт. Times New Roman. Одинарний інтервал. Робота складається з: - титул – 1 с.; - зміст – 2 с.; - вступ: актуальність, об'єкт, предмет, мета та завдання дослідження. - основна частина: не менше 2 розділів. - висновки формуються відповідно до завдань. **Критерії оцінювання захисту РГР.** *Стартовий бал 15.* Захист РГР триває не більше 10 хвилин. Якщо при захисті доповідач вклався в час, але не розкрив тему, нараховуються мінус бали (залежно від повноти розкриття). За неправильну відповідь на запитання мінус 2 бала, а за неповну відповідь мінус 1 бал. За відсутність презентації мінус 2 бали.
Лабораторні роботи	**Критерії оцінювання лабораторних робіт** 1. Підготовленість до лабораторних занять 2. Самостійність виконання практичних робіт. 3. Повнота розкриття теми. 4. Своєчасність виконання практичних робіт
Умови допуску до підсумкового контролю	Позитивна оцінка за всіма обов'язковими видами робіт (практичні роботи та РГР)

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки лабораторних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Чернігівського національного технологічного університету та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положення про організацію освітнього процесу в ЧНТУ.

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням.

8. Рекомендована література

Базова

1. Информационное противоборство в современных условиях: [Монография] / Л.Г. Пирцхалава, В.А. Хорошко, Ю.Е. Хохлачева, М.Е. Шелест / Под ред. профессора В.А. Хорошко. – К.: ЦП «Компринт», 2019. – 226 с.
2. Информационно-психологическая безопасность в зпоху глобализации : учеб. пособ. / [В.М.Петрик, В.В.Остроухов, А.А.Штоквиш и др.] ; под. ред. В.В.Остроухова. - К., 2008. - 544 с.
3. Інформаційна безпека (соціально-правові аспекти) : підруч. / [В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк та ін.] ; за ред. Є.Д.Скулиша. - К.:КНТ, 2010.-776 с.
4. Інформаційна безпека держави: підручник / [В.М.Петрик, М.М.Присяжнюк, Д.С.Мельник та ін.]; в 2 т. / – К. : Вид-во ІСЗЗІ НТУУ “КПІ”, 2016. – *Т. 1*. – 264 с.
5. Інформаційно-психологічне протиборство (еволюція та сучасність): навч. посіб. / Я.М.Жарков, В.М.Петрик, М.М.Присяжнюк та ін. - К.: ЗАТ "ВІПОЛ", 2013.-246 с.
6. Інформаційно-психологічне протиборство : підручник. Видання третє доповнене та перероблене / [В.М.Петрик, В.В.Бедь, М.М.Присяжнюк та ін.]; за заг. ред. В.В.Бедь, В.М.Петрика. - К.: ПАТ «ВІПОЛ», 2018. - 388 с.
7. Історія інформаційно-психологічного протиборства : підруч. / [Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш] ; за заг. ред. Є.Д.Скулиша. - К. : Наук.-вид. відділ НА СБ України, 2012.-208 с.
8. Петрик В.М., Бакалинський О.О., Жарков Я.М. та ін. Інформаційно-психологічне протиборство (еволюція та сучасність) : навч. посіб. – К.: Вид-во ІСЗЗІ НТУУ “КПІ”, 2012. – 248 с.
9. Петрик В.М., Присяжнюк М.М., Мельник Д.С. та ін. Забезпечення інформаційної безпеки держави: підручник ; за заг. ред. О.А.Семченка та В.М.Петрика. – К.: ДНУ «Книжкова палата України», 2015. – 672 с.
10. Соціальна інженерія (системний аналіз): навч. посіб. / за заг. ред. В.І.Курганевича та В.М.Петрика. – К., 2019. – 200 с.
11. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. / [О.М.Богданов, В.М.Петрик, Д.В.Пахольченко] / за заг. ред. В.М.Петрика. – К., 2018. –80 с.
12. Соціальна інженерія в контексті кібернетичної безпеки України (сучасні технології та шляхи захисту): навч. посіб. / [Ю.Г.Куцан, О.М.Богданов, В.М.Петрик, Д.В.Пахольченко, А.В.Давидюк] / за заг. ред. В.М.Петрика. – К., 2017. – 80 с.
13. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева та ін.] ; за заг. ред. Є.Д.Скулиша. - К.: Наук.-вид. відділ НА СБ України, 2010. - 248 с.

Допоміжна

1. Ажмухамедов Н.М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования. – Астрахань: АГТУ, 2012. – 344 с.

2. Андреева Г.М. Социальная психология. – М. Аспект- Пресс, 2014. – 363 с.

3. Безбах В.Г., Онищук М.І. Протидія інформаційно-психологічному впливу противника: навч.-метод. посібник. – К.: НАОУ, 2002. – 40 с.

4. Бірюков В.О., Есаулов М.Ю., Жук П.В., Міночкін А.І., Павлов І.М. Теоретичні основи інформаційної боротьби в сучасних війнах, воєнних конфліктах та у війнах майбутнього. – К.: ВІТІ ДУТ, 2013. – 322 с.

5. Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. Теоретико-методологічні основи забезпечення національної безпеки України: Теоретичні основи, методи й технології забезпечення національної безпеки України. – К.: Наук. вид. від НА СБУ, 2012. – 548 с.

6. Бурячок В.Л., Хорошко В.О. Технологія прийняття рішень у складних соціотехнічних системах – К.: ДУІКТ, 2012. – 344 с.

7. Бурячок В.Л, Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки. – К: ПВП «Задруга», 2014. – 222 с.

8. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. – К.: ДУТ, 2015. – 288 с.

9. Вепринцев В.Б., Манойло А.В. Петренко А.Й., Фролов Д.Б. Операции информационно-психологической войны и краткий энциклопедический словарь-справочник. – М.: Горячая линия-Телеком, 2005. – 495 с.

10. Горбулін В.П., Биченюк М.М. Проблеми захисту інформаційного простору України. – К.: Інтертехнологія, 2009. – 136 с.

11. Доктрина інформаційної безпеки України (затверджена указом Президента України №47/2017 від 25.02.2017 р.)

12. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. – К.: НІСД, 2011. – 30 с.

13. Еременко В.Т., Першуков В.Н., Пикалов Б.В., Третьяков О.В. Актуальные проблемы информационного противоборства в социотехнических системах. – Орел: Изд. Госуниверситет УНПК, 2015. – 291 с.

14. Жарков Я.М. та інші. Інформаційно-психологічне протиборство (еволюція та сучасність). – К.: Віпол, 2013. – 247 с.

15. Закон України «Про основи національної безпеки України».

16. Інформаійна безпека держави у контексті протидії інформаційним війнам: навч. посібник / За ред. В.Б. Толубко. – К: НАОУ, 2004. – 176 с.

17. Інформаційна безпека: підручник / Острухов В.В., Петрик В.М., Присяжнюк М.М. та інші. – К.: КНТ, 2010. – 776 с.

18. Кара-Мурда С.Г. Манипуляция сознанием. – М.: Изд. «Алгоритм», 2000. – 464 с.

19. Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры. – СПб: БХВ-Петербург, 2007. – 368 с.

20. Леонтьєва А.Є. Пропаганда, як інформаційно-психологічний складник політичних процесів. – Львів: ЛНУ ім. І. Франка, 2004. – 298 с.

21. Литвиненко О.В. Інформаційні впливи і операції. Теоретико-аналітичні нариси. – К.: НІСД, 2003. – 240 с.

22. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. – СПб: Наукоемкие технологии, 2017. – 546 с.

23. Месснер Е.Э. Мятеж-имя третьей всемирной. – Буэнос-Айрес, 1960. – 480 с.

24. Месснер Е.Э. Хочешь мира, победи мятеж-войну. – М.: Воен. Университет, Русский путь, 2005. – 485 с.

25. Нарис теорії і практики інформаційно-психологічних операцій / Дзюба М.Т., Жарков Я.М., Ольховой І.О., Онищук М.І. // За заг. ред. В.В. Балабіна. – К.: ВІТІ НТУУ «КПІ», 2006. – 472 с.

26. Нилус С.А. Протоколы Сионских Мудрецов: Всемирный тайный заговор / Изд. Берлинъ, 1922. – 125 с. 222

27. Панарин И.Н. Технология информационной войны. – М.: Изд. Мир безопасности, 2003. – 320 с.

28. Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення. – Харків: Цифрова друкарня №1, 2013. – 270 с.

29. Пєвцов Г.В., Пєвцов Г.В, Черкасов О.М. – Забезпечення інформаційної безпеки регіону: проблема, концепція та шляхи її реалізації. – Харків: Вид. Харт НАДУ «Магістр», 2008. – 138 с.

30. Світова гібрідна війна: український фронт / за заг. ред. В.П. Горбуліна. – К.: НІСД, 2017. – 496 с.

31. Технології розвитку і захисту національного інформаційного простору / О. Онищенко, В. Горовий, В. Попик та інші. – К.: НАН України, Нац. б-ка України ім. В.І. Вернадського, 2015. – 296 с.

32. Хорошко В.А., Шелест М.Е. Информационно-аналитическое обеспечение безопасности К.: ВПВ «Задруга», 2016. – 183 с.

33. Хорошко В.О., Грищенко І.С. Сучасне інформаційне протиборство: методи та засоби // Інформаційна безпека, №2(26), 2017. – С. 70-74.

34. Хорошко В.О., Грищук Р.В. Кібернетична зброя: класифікація, базові принципи побудови методи та засоби застосування й захист від неї // Сучасна спеціальна техніка, №4, 2016. – С.30-37.

35. Хорошко В.О., Хохлачова Ю.Є. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Частина 1 // Безпека інформації, Т22, №3, 2016. – С. 283-289.

36. Хорошко В.О., Шелест М.Е. Кибертерроризм и информационная безопасность // Правове, нормативне та методологічне забезпечення систем захисту інформації в Україні, Вип. 1(27), 2014. – С. 9-14.

37. Чалдин Р. Психология влияния. – СПб.:Питер, 2016. – 336 с.

38. Шиян А.А., Бурячок В.Л. Класифікація технологій для здійснення інформаційно-психологічного впливу на процес раціональної діяльності людини // Сучасний захист інформації, №1, 2014. – С. 64-70.

39. Штромайор Г. Політика: мас-медіа. – К.: Вид. дім «КиєвоМогилянська академія», 2008. – 303 с.

Інформаційні ресурси

Новітні теоретичні та практичні дані та матеріали? що стосуються теорії та практики захисту інформації рекомендується відслідковувати засобом звертання до наступних сайтів.

1. http://www.rsasecurity.com
2. http://www.nist.gov
3. http://www.eprint.iacr.org
4. http://www.citeseer.ist.psu.edu
5. http://www.ansi.org
6. http://www.cryptography.org
7. http://www.iso.org
8. http://www.linuxiso.org
9. http://www.cryptography.com
10. http://www.springerlink.com
11. http://www.cacr.math.uwaterloo.ca
12. http://www.financialcryptography.com
13. http://www.austinlinks.com
14. http://world.std.com/~franl/crypto.html
15. http://www.cryptonessie.org
16. http://www.cryptography.ru
17. http://www.osti.gov/eprints
18. http://www.intel.com
19. http://www.msdn.com
20. http://www.ph4s.ru/book_kripto.html