Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра теорії та практики управління

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Робоча програма навчальної дисципліни (Силабус)

1. Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*28 Публічне управління та адміністрування*
Спеціальність	*281 Публічне управління та адміністрування*
Освітня програма	***Адміністративний менеджмент, Електронне урядування***
Статус дисципліни	*Обов'язкова*
Форма навчання	*Очна / заочна*
Рік підготовки, семестр	*3 курс, осінній семестр*
Обсяг дисципліни	*90 год (3 кредити ЄКТС)*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	*rozklad.kpi.ua* *Денна форма: лекції раз на два тижні, семінари – раз на тиждень* *Заочна форма: 8 годин лекцій та 6 годин семінарських/практичних занять*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Архипова Євгенія Олександрівна, к.філос.н., доцент (лекції, семінарські/практичні)* *evgar55@gmail.com*
Розміщення курсу	Google classroom

2. Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Навчальна дисципліна орієнтована на формування у студентів розуміння інформаційної безпеки як складного багаторівневого явища, що має соціальні, психологічні й технічні виміри. Результатом вивчення дисципліни є формування та/або розвиток навичок виявлення і протидії інформаційним загрозам на рівні людини, суспільства та держави. Здобувачі вищої освіти також вивчатимуть положення нормативно-правових актів, які спрямовані на забезпечення інформаційних прав та свобод людини і громадянина та захист інтересів держави в інформаційній сфері.

Метою навчальної дисципліни є формування[1] таких програмних компетентностей та програмних результатів навчання:

[1] мається на увазі, що цей освітній компонент забезпечує формування даних компетентностей та програмних результатів навчання разом із іншими освітніми компонентами, визначеними в ОПП у Матриці відповідності програмних компетентностей компонентам освітньої програми та Матриці забезпечення програмних результатів навчання відповідними компонентами освітньої програми.

- програмні компетентності:

1. (ЗК2)[2] Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
2. (ЗК3) Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
3. (ФК3) Здатність забезпечувати дотримання нормативно-правових та морально-етичних норм поведінки.

- програмні результати навчання:

4. (18) Забезпечувати формування безпечних умов функціонування людини, суспільства, держави

Під час вивчення навчальної дисципліни здобувачі вищої освіти:

- отримають теоретичні знання щодо сутності та взаємозв'язків інформаційної безпеки, безпеки інформації, кібербезпеки та захисту інформації;

- розвинуть навички критичного ставлення до отримуваної інформації, що сприятиме збереженню та примноженню моральних, культурних, наукових цінностей і досягнень суспільства;

- розвинуть навички ідентифікації та оцінювання наслідків реалізації загроз у сфері інформаційної безпеки для життєдіяльності окремої особистості, груп людей, організацій та держави;

- отримають знання щодо значення інформаційної безпеки у контексті забезпечення національної безпеки України, ознайомляться з пріоритетними напрямами державної політики в інформаційній сфері;

- поглиблять знання нормативно-правових актів в частині, що регулюють інформаційні відносини у сфері публічного управління та адміністрування, зокрема щодо доступу громадян до інформації, яка знаходиться у розпорядженні органів державної влади;

- розвинуть навички забезпечення захисту приватності в повсякденному житті та професійній діяльності;

- поглиблять теоретичні знання та розвинуть практичні навички щодо використання маніпулятивних прийомів впливу на індивідуальну та масову свідомість;

- отримають базові знання щодо інформаційного протиборства, інформаційної війни, гібридної війни та спеціальних інформаційних операцій.

Навчальна дисципліна орієнтована на розвиток загальної інформаційної культури, критичного мислення та громадянської свідомості студентів, а також на формування професійних знань фахівців з публічного управління та адміністрування у сфері інформаційної безпеки.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

За структурно-логічною схемою підготовки фахівця дана навчальна дисципліна пов'язана з такими дисциплінами циклу професійної підготовки, як «Публічна служба», «Основи публічного управління та адміністративної діяльності», «Основи електронного урядування». Отримані теоретичні знання

[2] у дужках після номеру подано шифр компетентності чи результату навчання згідно з ОПП.

та практичні навички сприяють кращому розумінню дисциплін, що вивчатимуться пізніше, зокрема дисциплін «Державні інформаційні ресурси», «Соціальна інженерія: технології взаємодії влади і громади» та деяких дисциплін вільного вибору («Стратегії та технології мережевих війн», «Електоральні технології»).

3. Зміст навчальної дисципліни

Тема 1 Інформаційна безпека як складова національної безпеки

Тема 2. Інформація та інформаційне суспільство

Тема 3. Інформаційна безпека та безпека інформації. Загрози в інформаційній сфері

Тема 4. Кібернетична безпека.

Тема 5. Захист приватності.

Тема 6. Маніпулювання інформацією.

Тема 7. Інформаційне протиборство та інформаційні війни.

4. Навчальні матеріали та ресурси

Основна:

Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1,11 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с. Режим доступу: https://ela.kpi.ua/handle/123456789/43377

Богуш В.М., Юдін О.К. Інформаційна безпека держави. – К.: МК-Прес, 2005. – 432с. – Режим доступу: http://www.ex.ua/72793518

Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с. . – Режим доступу: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

Кормич Б.А. Інформаційна безпека: організаційно-правові основи. – К.: Кондор, 2008. – 384 с.

Допоміжна:

Архипова Е.А. Социальная составляющая информационной безопасности / Е.А. Архипова // Безпека інформації: Наук.-практ. журнал. – 2012. – Том 18, № 2 (2012). – С.28-32.
Архипова Є.О. Синергетичний вектор дослідження безпеки в сучасному суспільстві / Є.О. Архипова // Вісник Національного технічного університету України „КПІ”. Філософія. Психологія. Педагогіка. – 2014. – 1 (40)/2014 – С.3-9. http://journal-phipsyped.kpi.ua/article/view/28286
Архипова Є.О. Теоретична сутність та практика використання асиметричної відповіді в умовах гібридної агресії / Є.О. Архипова // Інвестиції: практика та досвід. – 2016. – №24. – С. 125-129. http://www.investplan.com.ua/?op=1&z=5311&i=25

Інформація про інші основні та додаткові матеріали або посилання на матеріали чи ресурси, потрібні для вивчення навчальної дисципліни, публікується у гугл-класі.

3. Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Завдання та методичні рекомендації до виконання практичних робіт, питання до МКР, підсумкового контролю та інші матеріали викладаються в гугл-класі.

Орієнтовні плани лекційних та практичних занять також наведені в додатку А.

6. Самостійна робота студента

Питання до самостійного опрацювання для студентів денної форми навчання зазначені в планах лекційних та практичних занять.

Студенти заочної форми навчання опановують самостійно весь матеріал, який не було розглянуто на лекціях, але винесено на підсумковий та модульний контроль (див. додаток Б).

4. Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Система оцінювання орієнтована на отримання балів за засвоєння теоретичних знать, розвиток практичних умінь та навичок, а також на стимулювання активності студентів на заняттях. Вітається вільне висловлювання студентами своєї позиції щодо питань, які розглядаються на заняттях, та самостійний пошук додаткової інформації. Відносини між студентами та викладачем здійснюється на партнерських началах.

Студенти можуть ініціювати внесення окремих питань/тем до розгляду на заняттях.

Основні матеріали або посилання на матеріали чи ресурси, потрібні для вивчення навчальної дисципліни, розміщуються у Google class. Матеріали чи ресурси для додаткового/поглибленого вивчення окремих питань розміщуються на Google-диску та/або шукаються студентами самостійно, що забезпечує розвиток навичок пошуку інформації та її критичного аналізу.

Відвідування занять

Сам факт ***відвідування*** лекцій та семінарів може фіксуватися, але не оцінюється. Оцінюється виключно робота, яку студенти виконують на заняттях (зокрема, відповіді на семінарських заняттях, виконання контрольних та самостійних робіт). Невиконання студентами цих видів робіт може призвести до порушення умов РСО та виникнення академічної заборгованості. Студентам також рекомендується відвідувати заняття, оскільки на них пояснюється теоретичний матеріал, розбираються та аналізуються практичні роботи, що сприяє кращому розумінню матеріалу студентами.

Пропущені контрольні заходи

Пропущені ***самостійні роботи та експрес-контрольні*** у формі відкритих питань не відпрацьовуються. Можливо отримання балів за виконання протермінованих / пропущених контрольних заходів, якщо вони проводились у формі закритих тестів (у такому разі доступ до тесту надається в індивідуальному порядку).

Альтернативою ***відповіді*** на семінарському занятті є написання есе **(не більше 1)** та ***тестів-відпрацювань***. Якщо студент претендує на високу оцінку, альтернативні види робіт мають бути здані не пізніше, ніж за 2 дні після відповідного семінару. Для отримання атестації чи допуску до

семестрового контролю дозволяється здавати ці роботи пізніше. Відпрацювання «оптом» в кінці семестру не схвалюються, але дозволяють вийти на найменшу позитивну оцінку. Прийом будь-яких відпрацювань припиняється за 5 днів до заняття, на якому проводиться залікова контрольна робота.

Вимоги до есе – не менше 95 % унікальності.

Вимоги до тестів-відпрацювань:

- не менше 4 варіантів відповідей для питань з однією правильною відповіддю;
- не менше 6 варіантів відповідей для питань з двома чи більше правильних відповідей;
- не більше 2 відкритих питань, відповіді на такі питання мають піддаватись формалізації;
- правильні відповіді мають бути позначені / наведені.

Детальніше вимоги щодо тестів-відпрацювань викладені в окремому документі, який доступний для ознайомлення в гугл-класі.

Способи ліквідації заборгованостей, які виникли через певні форс-мажорні обставини у студентів, обговорюються в індивідуальному порядку.

Засоби комунікації

Каналами зв'язку є:

- повідомлення через гугл-клас (загальна інформація з дисципліни, завдання, матеріали, особисті повідомлення);
- месенджери Viber та Telegram (особисті повідомлення, оперативний зв'язок);
- пошта групи та особиста пошта викладача (резервний спосіб зв'язку).

Процедура оскарження результатів контрольних заходів

Студенти (індивідуально чи групою) мають можливість порушити будь-яке питання, яке стосується процедури проведення чи оцінювання контрольних заходів, і розраховувати на неупереджений його розгляд.

Календарний рубіжний контроль

Проміжна атестація студентів є календарним рубіжним контролем. Метою проведення атестації є підвищення якості навчання студентів та моніторинг виконання графіка освітнього процесу студентами

Академічна доброчесність та норми етичної поведінки

Політика та принципи академічної доброчесності, норми етичної поведінки студентів та викладачів визначені у Кодексі честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code .

Робота, у якій виявлено порушення принципів академічної доброчесності, не приймається. За таку роботу бали анулюються, а також можуть бути нараховані штрафні бали.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: відповіді на семінарських заняттях, експрес-опитування, МКР, ДКР.
Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

Семестровий контроль: залік

Рейтингова система оцінювання (денна форма навчання)

Рейтинг студента з навчальної дисципліни складається з балів, які він отримує за:

№ з/п	Контрольний захід оцінювання	Ваговий бал	Кіл-ть	Всього
1.	**Активність на семінарі** В т.ч.: - доповідь на семінарі - участь у обговореннях	**до 4,5** 3 1,5 (2)	 18	**36** до 21 до 36
2.	Самостійні роботи (експрес-контроль)	2-6		24
3.	МКР (тест)	20	1	22
4.	Домашня контрольна робота	18	1	18
	Всього			**100**

Система рейтингових (вагових) балів та критерії оцінювання

1. ***Активність на семінарах.*** *Максимальна сума балів за семінар – 4,5, за семестр – 36.*

Студенти можуть довільно комбінувати обидва різновиди активностей, використовуючи оптимальну для себе стратегію набрання балів.

Види активності на семінарі:

1.1. Доповідь

У кожній доповіді розкривається одне питання, винесене на обговорення на семінарському занятті. Максимальна кількість балів за доповідь – 3 бали. Сума балів за доповіді не може перевищувати 21 бала.

Критерії оцінювання відповідей:

- *«відмінно»,* повна відповідь на поставлене питання; якісна презентація; студент вільно орієнтується в матеріалі, знає термінологію, наводить приклади – 2,5-*3 бали*;
- *«добре»,* відповідь потребує невеликих уточнень, студент знає матеріал, наводить шаблонні приклади – *2-2,5 бали;*
- *«задовільно»,* відповідь потребує суттєвих доповнень; студент плутається в термінології та не може відповісти на уточнюючі запитання, не може навести приклади – *1,5-2 бали*;
- *«незадовільно»,* відповідь не відповідає вимогам на 1,5 бали – *0 балів*.

1.2. Участь у обговореннях

Передбачає коментарі та доповнення основних доповідей, задавання питань доповідачу, ініціювання та участь в дискусіях тощо. За участь в обговореннях можна отримати до 1,5 балів за семінар (в окремих випадках – до 2 балів). Участь в обговореннях фіксується позначками «+», та переводитись у бали раз на 4-5 тижнів або ж бали виставляються кожне заняття, причому в кінці місяця та/або семестру можливе нарахування додаткових коригуючих балів.

2. ***Самостійні роботи (експрес-контроль)***

Проводяться за темою поточного чи попереднього семінарів у формі відкритих питань, завдань чи онлайн-тестування. Завдання та критерії оцінювання оголошуються безпосередньо перед контрольним заходом. В залежності від складності роботи максимальна оцінка складає від 2 до 6 балів. Орієнтовна кількість самостійних робіт та експрес-контролів – 7.

3. ***Модульна контрольна робота***

Ваговий бал – 22. Проводиться наприкінці семестру у формі тестування. В тесті використовуються закриті питання.

Якщо за МКР набрано менше 50% від максимального балу, вона вважається незарахованою та оцінюється в 0 балів.

4. ***Написання ДКР***

Метою ДКР є вивчення прийомів (технік) маніпулювання, розвиток практичних навиків їх викриття та ідентифікації в різних життєвих ситуаціях.

Ваговий бал – 18. Детальніше про ДКР – в додатку.

Штрафні та заохочувальні бали нараховуються за:

Заохочувальні бали нараховуються за:

- повідомлення на семінарському занятті за результатами опрацювання новітньої наукової літератури – 4 бали;
- участь в конференції (за тематикою дисципліни) – до 6 балів.
- публікація статті (за тематикою дисципліни) – до 10 балів (також можливе зарахування відповідних самостійних робіт чи доповіді, що обговорюється в індивідуальному порядку).

Штрафні бали нараховуються за роботи, в яких виявлено плагіат, а також за порушення термінів здачі робіт.

Атестація студентів проводиться двічі за навчальний семестр (на 8 та 14 тижнях). Студент є атестованим, якщо його поточний рейтинг складає не менше половини максимально можливого балу на момент виставлення атестації. Орієнтовні максимальні бали для першої та другої атестації - 30 та 70 відповідно.

Максимальна сума балів за семестр – 100. До заліку не допускаються студенти, семестровий рейтинг яких менше 40 балів та які не здали ДКР.

Для отримання заліку з навчальної дисципліни «автоматом» потрібно мати 1) рейтинг не менш ніж 60 балів, 2) зараховану ДКР. Студенти, які наприкінці семестру мають рейтинг менше 60 балів, а також ті, хто хоче підвищити оцінку у системі ECTS, пишуть заліковий тест. При цьому попередній рейтинг студента з навчальної дисципліни скасовується і він отримує оцінку з урахуванням результатів залікового тесту та балів за індивідуальне завдання, яка є остаточною.

Обов’язкові умови допуску до залікової контрольної роботи		Критерій
1	Семестровий рейтинг	Не менше 40 балів
2	Зарахована ДКР	+

Заліковий тест містить 40 закритих запитань, які формулюються на основі матеріалу, розглянутого на лекціях та семінарах. Максимальна оцінка за заліковий тест складає 82 бали. 82 бали (тест) + 18 балів (ДКР) = 100 балів.

Критерії оцінювання залікового тесту наступні:

- «відмінно» отримує студент, який дав правильні відповіді не менше, ніж на 90 % запитань (36 правильних відповідей) – 74-82 бали;
- «добре» отримує студент, який дав правильні відповіді не менше, ніж на 75 % запитань (30 правильних відповідей) – 61-73 бали;
- «задовільно» отримує студент, який дав правильні відповіді не менше, ніж на 60 % запитань (24 правильних відповідей) – 49-60 балів;
- «незадовільно» отримує студент, який правильно відповів менше ніж на 60% запитань – 0 балів.

Підсумкова оцінка формується шляхом переведення суми балів, отриманих за:

- семестрові завдання (для тих, хто отримує залік «автоматом») або
- заліковий тест та індивідуальне семестрове завдання (ДКР) (для тих, хто складав залік)

згідно з таблицею, наведеною нижче.

Рейтингова система оцінювання (заочна форма навчання)

Рейтинг студента з дисципліни складається з балів, які він отримує за:

1) ДКР;
2) робота на семінарських заняттях;
3) заліковий тест.

Система рейтингових (вагових) балів та критерії оцінювання

1. ***Домашня контрольна робота (ДКР)***

Максимальна кількість балів за ДКР – 30 балів.

Критерії оцінювання:

- *«відмінно»,* завдання виконані повною мірою, (не менше 90% потрібної інформації), робота написана самостійно, відповідає встановленим вимогам та здана вчасно – *28 -30 балів*;
- *«добре»,* завдання виконані досить повно (не менше 75% потрібної інформації), наявні незначні відхилення від встановлених вимог, здана вчасно – *24 - 26 балів*;
- *«задовільно»,* завдання виконані погано та/або наявні суттєві відхилення від встановлених вимог та/або робота здана із суттєвою затримкою – 20 - *22 балів*;
- «незадовільно», робота не відповідає вимогам на 20 балів – *0 балів*.

Термін здачі ДКР - не пізніше ніж за 5 днів до семінару з цієї дисципліни на заліковій сесії.

2. ***Робота на семінарських заняттях***

В плані 3 семінарських заняття, за які сумарно можна отримати до 20 балів.

Види робіт на семінарі: доповідь з презентацією, участь у обговореннях, відповіді на питання, самостійна робота.

3. ***Заліковий тест***

Заліковий тест містить 50 закритих запитань, які формулюються на основі матеріалу, зазначеного у програмі. Кожна правильна відповідь оцінюється у 1 бал. Максимальна оцінка за заліковий тест складає 50 балів.

30 балів (ДКР) + 20 балів (робота на семінарах) + 50 балів (тест) = 100 балів.

Штрафні та заохочувальні бали нараховуються за:

Штрафні бали передбачені за невчасно здану ДКР

Заохочувальні бали

- повідомлення на семінарському занятті за результатами опрацювання новітньої наукової літератури – 3 бали;
- доповідь на Днях Науки – 3 бали.
- проходження онлайн-курсів за тематикою дисципліни (див. п.9) – до 5 балів за сертифікат.

Загальна кількість заохочувальних балів не може перевищувати 10.

Максимальна сума балів складає 100. До заліку не допускаються студенти, які не здали ДКР.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Онлайн-курси

Визнання результатів навчання, набутих через неформальну освіту, здійснюється у відповідності до Положення. За проходження онлайн-курсів за тематикою дисципліни (за умови пред'явлення відповідного сертифікату, отриманого в цьому семестрі) студенту можуть бути зараховані бали за виконання певних поточних завдань або нараховані заохочувальні бали.

Деякі онлайн-курси за тематикою дисципліни:

Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні – https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IH101+2021_T3/about

Дезінформація: види, інструменти та способи захисту – https://courses.prometheus.org.ua/courses/course-v1:Prometheus+DISINFO101+2021_T2/about

Цифрова безпека та комунікація в онлайні – https://vumonline.ua/course/digital-security-and-communication-online/

Інклюзивне навчання

Навчальна дисципліна може викладатися для всіх студентів з особливими освітніми потребами. У разі потреби завдання можуть бути скориговані.

Робочу програму навчальної дисципліни (силабус):

Складено:

доцент кафедри теорії та практики управління, кандидат філософських наук, доцент,
Архипова Євгенія Олександрівна

Ухвалено кафедрою теорії та практики управління (протокол № ___ від _____)

Погоджено Методичною комісією КПІ ім. Ігоря Сікорського (протокол № __ від _____)

1. Додаток А

Плани лекційних та практичних занять
А.1. Лекційні заняття (денна форма навчання)

Лекція 1. Інформаційна безпека як складова національної безпеки

2. Визначення та зміст поняття «інформаційна безпека».
3. Концепція національної безпеки України.
4. Роль та місце інформаційної безпеки в системі національної безпеки.
5. Захист життєво важливих інтересів держави в інформаційній сфері.

Завдання на СРС: надайте класифікацію національних інтересів.

Лекція 2. Інформація, інформаційні процеси і системи. Інформаційне суспільство

5. Інформація, інформаційні процеси і системи: основні поняття та визначення.
6. Види інформації
7. Життєвий цикл інформації.
8. Соціальна суть інформації.
9. Глобальний характер інформатизації.
10. Загрози та виклики інформаційного суспільства.

Дидактичні засоби: схема «Види інформації».

Завдання на СРС: визначте сутність поняття «амбівалентність інформації».

Лекція 3. Інформаційна безпека та безпека інформації

1. Відмінність понять інформаційна безпека та безпека інформації.
2. Основні напрямки інформаційної безпеки.
3. Інформаційне протиборство та конфлікти, інформаційна війна, інформаційна зброя.
4. Принципи, головні задачі та функції забезпечення захисту інформації.
5. Національна система захисту інформації.

Завдання на СРС: охарактеризуйте стан та проблеми внутрішніх та зовнішніх відносин в інформаційній сфері.

Лекція 4. Кібернетична безпека

1. Поняття кібернетичної безпеки. Підходи до визначення кібернетичної безпеки.
2. Співвідношення термінів «кібербезпека» та «інформаційна безпека».
3. Стратегія кібербезпеки України.
4. Загрози кібербезпеці та загрози критичній інфраструктурі. Точки перетину. Кіберзлочин та кіберзлочинність.

Завдання на СРС: знайдіть в наукових джерелах визначення кібербезпеки та кіберзагроз та проаналізуйте ці визначення.

Лекція 5. Персональні дані

1. Нормативно-правова база у сфері захисту персональних даних.

2. Персональні дані як об’єкт захисту. Персональних дані та конфіденційна інформація.
3. Суб'єкти відносин, пов'язаних із персональними даними. Їх права та обов’язки.
4. Вимоги до обробки персональних даних.

Завдання на СРС: Визначте, які дані відносяться до чутливих персональних даних.

Лекція 6. Право на приватність та його захист

1. Розвиток уявлень про право на приватність (приватне життя) та захист приватності.
2. Зміст поняття «персональні дані». Види персональних даних.
3. Міжнародні акти із захисту персональних даних та захисту приватності.
4. Вітчизняні нормативно-правові акти із захисту персональних даних та приватного життя.
5. Захист приватності в Інтернеті.

Завдання на СРС: Визначте внесок статті С. Уоррена та Л. Брандейса «Право на приватність» у розумінні питання захисту приватності.

Лекція 7. Маніпулювання

1. Сутність, особливості та причини маніпулювання інформацією.
2. Підготовка та проведення маніпуляцій інформацією.
3. Основні засоби маніпуляції суспільною свідомістю.
4. Прийоми і технології маніпулювання при особистому спілкуванні.
5. Способи маніпулювання в мас-медіа.

Завдання на СРС: пошук підзаконних актів з регулювання інформаційних відносин в певній сфері діяльності.

Лекція 8. Інсайдерство та соціальна інженерія

1. Інсайдерство та інсайдери. Види інсайдерів.
2. Соціальна інженерія: зміст поняття.
3. Приклади реалізації соціоінженерних атак.

Завдання на СРС: Кевін Мітник про соціальну інженерію.

Лекція 9. Інформаційне протиборство та інформаційна війна

1. Інформаційне протиборство та його види.
2. Інформаційна війна. Інформаційна зброя.
3. Поняття гібридної війни та гібридної агресії.
4. Спеціальні інформаційні операції.

Завдання на СРС: Наведіть історичні приклади гібридних війн.

А.2. Практичні (семінарські) заняття (денна форма навчання)

Семінарське заняття 1. Вступ до інформаційної безпеки

1) Проблеми розуміння інформаційної безпеки в професійних колах та на рівні суспільної свідомості.
2) Інформаційна безпека як складова національної безпеки.
3) Інформаційна безпека та безпека інформації.
4) Соціальні аспекти інформаційної безпеки.
5) Загальне розуміння технічних аспектів інформаційної безпеки.

Завдання на СРС: Перелічіть загрози інформаційній безпеці особи.

Семінарське заняття 2. Державна інформаційна політика

1. Національний інформаційний суверенітет.
2. Сутність та завдання національної інформаційної політики.
3. Державна інформаційна політика України.
4. Інформаційна політика зарубіжних країн.
5. Захист життєво важливих інтересів держави в інформаційній сфері.
6. Інтереси людини та суспільства в інформаційній сфері.

Завдання на СРС: Розкрити основні положення ЗУ «Про Національну програму інформатизації».

Семінарське заняття 3. Інформація, інформаційні процеси і системи

1. Сутність та види інформації.
2. Атрибутивна та функціональна концепції інформації
3. Соціальна інформація та її характеристики.
4. Міри інформації
5. Проблеми визначення цінності інформації.
6. Інформаційні процеси і системи: основні поняття та визначення.
7. Сутність та значення інформаційних революцій для розвитку людства.

Завдання на СРС: Порівняйте поняття «цінність інформації» та «корисність інформації». В чому полягає глобальний характер інформатизації? Визначте поняття «сучасні інформаційні системи».

Семінарське заняття 4. Інформаційне суспільство та суспільство знань

1. Становлення та розвиток концепцій інформаційного суспільства (Д.Белл, М. Кастельс, Е. Тоффлер, В. Іноземцев та ін) – доповіді за окремими авторами.
2. Суспільство знань: основні риси та тенденції.
3. Загрози та виклики інформаційного суспільства.

Завдання на СРС: Інформаційне суспільство у працях соціальних філософів.

Семінарське заняття 5-6. Інформаційна безпека та безпека інформації. Загрози в інформаційній сфері

1. Особливості розуміння термінів «інформаційна безпека», «безпека інформації», «захист інформації».
2. Відмінність інформаційної безпеки та безпеки інформації, їх основні складові.
3. Основні визначення поняття «загроза». Визначення і джерела інформаційних загроз.
4. Класифікація інформаційних загроз.
5. Загрози інформаційній безпеці людини.
6. Загрози інформаційній безпеці суспільства.
7. Загрози інформаційній безпеці держави.
8. Загрози безпеці інформації. Основні загрози доступності, цілісності та конфіденційності.
9. Гучні приклади порушення інформаційної безпеки.

Завдання на СРС: приклади загроз доступності та цілісності інформації.

Семінарське заняття 7-8. Кібернетична безпека, кіберзагрози та кіберзахист

1. Поняття кібернетичної безпеки. Підходи до визначення кібернетичної безпеки. Співвідношення термінів «кібербезпека» та «інформаційна безпека».
2. Кіберпростір та інформаційних простір: критерії розмежування.
3. Об’єкти та суб’єкти забезпечення кібербезпеки.
4. Загрози кібербезпеці та загрози критичній інфраструктурі. Точки перетину. Кіберзлочин та кіберзлочинність.
5. Пріоритети та напрями забезпечення кібербезпеки України.
6. Національні стратегії кібербезпеки інших країн (доповіді за країнами).

Завдання на СРС: Кореляція загроз кібернетичній безпеці із інформаційними загрозами людині, суспільству та державі.

Семінарське заняття 9. Захист приватності

1. Зміст та обсяг поняття «персональні дані».
2. «Чутливі» персональні дані та їх обробка.
3. Доступ до персональних даних.
4. Розвиток уявлень про право на приватність (приватне життя) та захист приватності.
5. Складнощі визначення поняття приватного життя.
6. Основні категорії та терміни в сфері захисту персональних даних.
7. Організація захисту персональних даних.
8. Міжнародні акти із захисту персональних даних та захисту приватності.
9. Вітчизняні нормативно-правові акти із захисту персональних даних та приватного життя.

Завдання на СРС: проблеми захисту права на приватність користувачів інтернету.

Семінарське заняття 10. Захист приватності в мережі

1. Ризики приватності в інтернеті.
2. Захист права на приватність користувачів інтернету.
3. Налаштування приватності в популярних браузерах.
4. Особливості спілкування в соціальних мережах та правила листування електронною поштою.
5. Дискусія: чи можливо забезпечити приватність в інтернеті?

Завдання на СРС: проблеми захисту права на приватність користувачів інтернету.

Семінарське заняття 11. **Маніпуляції свідомістю**

1. Поняття та ознаки маніпулювання.
2. Підготовка та реалізація маніпуляцій.
3. Прийоми (техніки, технології) маніпулювання індивідуальною свідомістю
4. Прийоми (техніки, технології) маніпулювання масовою свідомістю
5. Маніпуляції в рекламі.

Семінарське заняття 12. Інсайдерство та соціальна інженерія

1. Соціальна інженерія та соціальні хакери: зміст понять.
2. Методи соціальної інженерії
3. Алгоритм соціотехнічної атаки
4. Типи соціоінженерних атак та приклади реалізованих атак (аналіз сміття; особистісні підходи; реверсивна соціальна інженерія; фішинг, вішинг, смішинг, фармінг тощо. Можна декілька доповідачів
5. Приклади соціального програмування
6. Інсайдерство та інсайдери. Види інсайдерів.
7. Витоки інсайдерської інформації (приклади). Захист від інсайдерських витоків інформації.

Завдання на СРС: проблеми захисту права на приватність користувачів інтернету.

Семінарське заняття 13-14. Інформаційне протиборство та інформаційна зброя

1. Основні поняття інформаційного протиборства: інформаційні протиборство, війна, тероризм, злочинність.
2. Інформаційне протиборство як форма забезпечення інформаційної безпеки
3. Визначення інформаційної війни
4. Концепція інформаційної війни
5. Органи інформаційної війни
6. Основні форми інформаційної війни
7. Визначення, особливості та сфера застосування інформаційної зброї
8. Інформаційна зброя воєнного застосування
9. Інформаційна зброя воєнного та невоєнного застосування
10. Особливості, що характеризують основні риси застосування інформаційної зброї

Завдання на СРС: основні форми інформаційної війни на державному рівні

Семінарське заняття 15. Інформаційна боротьба та психологічна війна

1. Заходи і способи інформаційної боротьби
2. Форми ведення інформаційної боротьби
3. Методологія оцінки ефективності інформаційної боротьби
4. Цілі та завдання психологічної війни
5. Види та закономірності психологічних впливів
6. Види психологічних впливів
7. Основи психологічних операцій

8. Зміст психологічних операцій та ефективність психологічного впливу в них
9. Форми психологічної війни.

Завдання на СРС: механізм реалізації психологічного впливу. Закономірності психологічного впливу

Семінарське заняття 16. Спеціальні інформаційні операції

1. Сутність та завдання спеціальних інформаційних операцій (СІО).
2. Види СІО (спрямовані проти суб'єктів, які ухвалюють рішення; спрямовані на компрометацію, завдання шкоди опонентам; спрямовані на політичну (економічну) дестабілізацію).
3. Методи СІО: дезінформування; пропаганда; диверсифікація суспільної свідомості; психологічний тиск; розповсюдження чуток.
4. Практичний досвід проведення СІО (доповіді за різними СІО).

Завдання на СРС: Порівняйте СІО, які проводяться на макро- і мікрорівні.

Семінарське заняття 17. Модульна контрольна робота

1) Закон України „Про інформацію":

- поняття інформаційних відносини, інформаційної діяльності, джерел інформації;
- право власності на інформацію, інформація як товар;
- доступ до інформації, поділ інформації за режимом доступу, інформація з обмеженим доступом;
- класифікація інформації за правовим режимом, правом власності, ступенем важливості.

2) Закон України «Про національну безпеку України» (в контексті ІБ).

3) Концепція інформаційної безпеки України (Проект).

Завдання на СРС: Проаналізувати різноманітні визначення інформації, національної безпеки.

Семінарське заняття 18. Підсумкове заняття

Доздача боргів, обговорення результатів ДКР підведення підсумків.

А.3. Лекційні та практичні (семінарські) заняття (заочна форма навчання)

Лекція 1. Інформаційна безпека як складова національної безпеки

1. Визначення та зміст поняття «інформаційна безпека». Відмінності від терміна «безпека інформації».
2. Концепція національної безпеки України.
3. Роль та місце інформаційної безпеки в системі національної безпеки.
4. Захист життєво важливих інтересів держави в інформаційній сфері.

Лекція 2. Кібернетична безпека

1. Поняття кібернетичної безпеки. Підходи до визначення кібернетичної безпеки.
2. Співвідношення термінів «кібербезпека» та «інформаційна безпека».
3. Стратегія кібербезпеки України.
4. Загрози кібербезпеці та загрози критичній інфраструктурі. Точки перетину. Кіберзлочин та кіберзлочинність.

Лекція 3. Персональні дані

1. Нормативно-правова база у сфері захисту персональних даних.
2. Персональні дані як об’єкт захисту. Персональних дані та конфіденційна інформація.
3. Суб'єкти відносин, пов'язаних із персональними даними. Їх права та обов’язки.
4. Вимоги до обробки персональних даних.

Лекція 4. Маніпулювання та соціальна інженерія

1. Сутність, особливості та причини маніпулювання інформацією.
2. Підготовка та проведення маніпуляцій інформацією.
3. Основні засоби маніпуляції суспільною свідомістю.
4. Соціальна інженерія та соціальні хакери: зміст понять.
5. Методи соціальної інженерії та алгоритм соціотехнічної атаки

Семінарське заняття 1. Державна інформаційна політика

1. Національний інформаційний суверенітет.
2. Сутність та завдання національної інформаційної політики.
3. Державна інформаційна політика України.
4. Інформаційна політика зарубіжних країн.
5. Захист життєво важливих інтересів держави в інформаційній сфері.
6. Інтереси людини та суспільства в інформаційній сфері.

Семінарське заняття 2. Захист приватності

1. Зміст та обсяг поняття «персональні дані».
2. «Чутливі» персональні дані та їх обробка.
3. Доступ до персональних даних.
4. Розвиток уявлень про право на приватність (приватне життя) та захист приватності.
5. Організація захисту персональних даних.
6. Міжнародні акти із захисту персональних даних та захисту приватності.
7. Вітчизняні нормативно-правові акти із захисту персональних даних та приватного життя.
8. Ризики приватності в інтернеті. Захист права на приватність користувачів інтернету.

Семінарське заняття 3. Інформаційне протиборство та інформаційна зброя

1. Основні поняття інформаційного протиборства: інформаційні протиборство, війна, тероризм, злочинність.
2. Інформаційне протиборство як форма забезпечення інформаційної безпеки
3. Визначення інформаційної війни та її основні форми
4. Визначення, особливості та сфера застосування інформаційної зброї
5. Інформаційна зброя воєнного застосування
6. Інформаційна зброя воєнного та невоєнного застосування
7. Особливості, що характеризують основні риси застосування інформаційної зброї
8. Заходи і способи інформаційної боротьби
9. Основи психологічних операцій

6. Додаток Б

Орієнтовний перелік питань для підготовки до модульного та підсумкового контролю з дисципліни “Основи інформаційної безпеки”

1. Розкрийте сутність інформаційної безпеки як складової національної безпеки.
2. Поясніть, у чому полягає актуальність інформаційної безпеки в сучасному суспільстві.
3. Визначте основні напрями інформаційної політики України. Надайте коротку характеристику її нормативно-правового забезпечення.
4. Розкрийте поняття національного інформаційного суверенітету. Назвіть інструменти, які можуть використовуватися для його забезпечення.
5. Охарактеризуйте підходи до визначення поняття інформації. Назвіть види інформації.
6. Поясніть зміст атрибутивної та функціональної концепції інформації.
7. Розкрийте етапи життєвого циклу інформації.
8. Поясніть підходи до визначення цінності інформації.
9. Наведіть класифікацію інформації за видами, за порядком доступу, за ступенем секретності.
10. Охарактеризуйте сутність та значення інформаційних революцій для розвитку людства.
11. Визначте, у чому полягає глобальний характер інформатизації.
12. Надайте загальну характеристику концепцій інформаційного суспільства.
13. Охарактеризуйте основні риси та проблеми сучасного інформаційного суспільства.
14. Назвіть основні риси та тенденції розвитку суспільства знань. Порівняйте його із інформаційним суспільством.
15. Визначте сутність та наведіть класифікацію інформаційних загроз. Виокремте загрози, які характерні саме для сучасного інформаційного суспільства.
16. Надайте коротку характеристику загрозам інформаційної безпеки людини, суспільства та держави.
17. Порівняйте поняття “Інформаційна безпека”, “безпека інформації”, “кібернетична безпека”.
18. Назвіть складові інформаційної безпеки. Розкрийте соціальні аспекти інформаційної безпеки.
19. Розкрийте основні властивості інформації як об'єкту захисту.
20. Визначте сутність кібернетичної безпеки. Назвіть пріоритетні напрями забезпечення кібербезпеки в Україні.
21. Визначте зміст та критерії розмежування кіберпростору та інформаційного простору.
22. Поясніть зміст понять “кіберзлочин” та “кіберзлочинність”.
23. Розкрийте сутність персональних даних та захисту приватності. Поясніть співвідношення понять “персональні дані” та “конфіденційна інформація”.
24. Розкрийте права та обов'язки суб'єктів відносин, пов'язаних із персональними даними. Поясніть вимоги до обробки персональних даних.
25. Розкрийте зміст понять «приватність». Визначте спектр проблем захисту приватності.
26. Дайте визначення поняття “маніпулювання”. Назвіть ознаки маніпулювання.
27. Охарактеризуйте процес підготовки та реалізації маніпуляцій.
28. Розкрийте сутність та наведіть приклади використання технологій маніпулювання суспільною свідомістю.
29. Розкрийте сутність та наведіть приклади використання технологій маніпулювання індивідуальною свідомістю.
30. Поясніть зміст понять “соціальна інженерія” (як метод отримання інформації) та “соціальні хакери”, розкрийте алгоритм реалізації соціотехнічної атаки.
31. Охарактеризуйте методи соціальної інженерії. Розкрийте класифікацію та наведіть приклади соціоінженерних атак.
32. Поясніть сутність та механізми захисту від фішингу, вішингу, смішингу, фармінгу.
33. Розкрийте зміст поняття “інсайдерство”. Охарактеризуйте види інсайдерів.
34. Розкрийте зміст понять інформаційне протиборство, інформаційна війна, інформаційна зброя.

35. Надайте визначення, охарактеризуйте види та особливості інформаційної зброї.
36. Поясніть сутність і задачі спеціальних інформаційні операції. Аргументуйте відповідь прикладами.
37. Розкрийте технологію проведення спеціальних інформаційних операцій.
38. Поясніть сутність та особливості гібридної війни.

Домашня контрольна робота з дисципліни
“Основи інформаційної безпеки”

Опис роботи
Метою ДКР є вивчення прийомів (технік) маніпулювання, розвиток практичних навиків їх викриття та ідентифікації в різних життєвих ситуаціях.

Студенти повинні підібрати по 6 прикладів застосування різних маніпулятивних прийомів чи технік. Приклади повинні бути різнопланові (на основі відеоматеріалів, графічних, текстових матеріалів тощо; рекламні, новинні, освітні, розважальні матеріали, ток-шоу тощо).
Всі приклади мають бути реальні та свіжі. Наприклад, якщо ви аналізуєте рекламний текст, ця реклама має демонструватися зараз; новинний, інформаційний матеріал – не старше 10 днів. Виключення – міжособистісні маніпуляції: наводячи приклад міжособистісних маніпуляцій, можна використовувати змодельовані ситуації (не більше 1 з 6 необхідних прикладів).

Повторення одного прикладу (конкретного) стосовно одного маніпулятивного прийому (техніки) не дозволяється.
Робота виконується в спільному гугл-документі.

Структура відповіді
Кожний приклад маніпулятивного прийому складається з:

- наскрізної нумерації прикладу, прізвища студента, дати та часу внесення прикладу в документ;
- опису матеріалу, який містить маніпуляцію. Це може бути фрагмент (текст) промови чи стенограма виступу (можна доповнювати відео чи аудіозаписом), **текстовий** опис відеоряду (також можна додати посилання на відео), фрагмент тексту (для друкованих матеріалів), опис ситуації тощо. Опис матеріалу повинен пояснювати, яким чином в цьому випадку реалізований маніпулятивний прийом/техніка. Текстовий опис може бути доповнений ілюстративним матеріалом (фотографія, стоп-кадр, рекламний постер тощо), посиланням на відео (із вказаням таймінгу, якщо загальний обсяг відео великий). Джерело має бути чітко ідентифіковано (наприклад, виступ ПІБ в політичному ток-шоу “ХХХ” від 7.11.20; реклама кави “Nescafe” на Інтері).
- за необхідності можна надати додаткові коментарі.

Якщо ви першим ілюструєте якусь маніпулятивну техніку (прийом), потрібно навести її назву та коротко викласти її суть (оформлення за шаблоном нижче).
Можна створювати і нові групи прийомів (нумерація першого рівня), але такі групи не повинні допускати дублювання прийомів. Наприклад, якщо якась із маніпулятивних технік універсальна (використовується і в рекламі, і в новинах, і в ток-шоу, то слід обрати загальну рубрику – маніпуляції в ЗМІ; якщо ж даний прийом використовується тільки в рекламі, то обирайте/створюйте відповідну групу.

Зверніть увагу, що у одних і тих саме технік можуть бути різні назви, тому переглядайте, що створили до вас, і уникайте дублювань. Небажано наводити приклади на ті прийоми, на які є вже більше 8 прикладів.

Посилання на документ для спільної роботи буде надано перед початком виконання ДКР.

На початку документу розміщена реєстраційна форма, в якій слід зазначати номери ваших прикладів по мірі їх внесення в документ. Вносити всі приклади в один день не обов'язково.

Термін виконання роботи: від моменту розгляду теми «Маніпуляції» до 6.12.2021 (включно).

Оцінювання ДКР (денна форма навчання)
Ваговий бал – 18 балів.
Критерії оцінювання:

- «відмінно», приклади повною мірою ілюструють заявлені маніпулятивні прийоми та відповідають всім встановленим вимогам, ДКР виконана вчасно – 16-18 балів;
- «добре», деякі приклади потребують додаткових пояснень, уточнень або їх опис не повною мірою розкриває особливості вказаних маніпулятивних прийомів. Приклади вирізняються різноманітністю – 13-15 балів;
- «задовільно», приклади досить однотипні, або їх опис погано розкриває сутність деяких заявлених маніпулятивних прийомів, або прикладів замало, або ДКР зроблена із несуттєвою затримкою (до 3 днів включно) – 10-12 балів.
- «зараховано», приклади однотипні, або їх опис погано розкриває сутність заявлених маніпулятивних прийомів, або наведена недостатня кількість прикладів та/ або ДКР зроблена із суттєвою затримкою – 4-9 балів.
- «незадовільно» – ДКР не зараховано.

Шаблон оформлення:

1.1 Назва

Сутність прийому (коротко)

Приклад 1.1.1. Підготовлено: Петрова О.І., 07.12.2019, 20:40

Опис відеоряду (обов'язково текстовий, крім того можна додати посилання на відеозапис), стенограма розмови, фрагмент тексту (для текстових джерел), опис ситуації, фотографічний матеріал тощо.
За необхідності - ваш коментар, пояснення.

Приклад 1.1.2. Підготовлено:

Опис, коментар, пояснення.

1.2 Назва

Сутність прийому (коротко).

Приклад 1.2.1. Підготовлено:

Опис, коментар, пояснення.

Приклад 1.2.2. Підготовлено:

Опис, коментар, пояснення.

1. Маніпуляції через ЗМІ (ТБ, преса)

1.1. Анонімний авторитет

В повідомленні зазначається, що джерелом інформації є якась вагома особа, провідний фахівець у даній сфері тощо, причому її ім'я не називається.

Приклад 1.1.1. Підготовлено: Іваненко Я.А., 20.12.2019 01.10

https://kp.ua/life/653252-kosmos-eto-kryvoi-puzyr

В даному прикладі посилаються на результати дослідження "британських вчених". Їх зазначають, зазвичай, будь-де, особливо часто в рекламі, що зустрічається в інтернеті.

Британські вчені виступають якимись максимально розумними, а їх інформацію - достовірною, що і викликає довіру людей. Хоча що це за вчені ніхто навіть не здогадується, тому що імен ніколи не вказують.

Коментар [Є.О.]: У цьому випадку як раз є імена. В даному новинному матеріалі згадується ім'я керівника дослідження (Елеонора Ді Валентино), а також афіляція цих дослідників (Манчестерський університет). Пошук інших матеріалів за цією темою дозволяє досить швидко встановити й імена інших дослідників (наприклад, тут: https://profile.ru/news/scitech/discoveries/uchyonye-postavili-pod-somnenie-beskonechnost-vselennoj-193312/)

Приклад 1.1.2. Підготовлено:

Опис, коментар, пояснення.

1.2. Маніпуляція гострою назвою

Така маніпуляція відбувається за допомогою гучного та шокуючого заголовка статті, яка і змушує прочитати її – не таку і шокуючу по суті. А заголовок, на ділі, взагалі часто вирвано із контексту.

Приклад 1.2.1 Підготовлено Іваненко Я.А., 20.12.2019

https://hyser.com.ua/politics/122691-putin-napadet-na-4-ukrainskih-goroda-klimkin-nazval-mesta-gde-nachnutsya-boi

Заголовок вказує на те, що Путін почав активну війну (Путин нападет на 4 украинских города. Климкин назвал места, где начнутся бои). Через це виникає бажання прочитати більше. Насправді, після прочитаного, виходить, що це лише припущення, один із можливих сценаріїв розвитку подій.

1.3. Назва

Сутність прийому (коротко).

Приклад 1.3.1. Підготовлено:

Опис, коментар, пояснення.

2. Маніпуляції в рекламі (тільки в рекламі)

2.1. Авторитет

Товар рекламує популярна особистість: кіноактор, кумир молоді й так далі. Розрахунок на стереотип: «раз уже такі люди купують, то сумніватися нічого, треба брати». Коли товар рекламує відома публічна особистість, це викликає захопленість та впевненість в якості товару.

Приклад 2.1.1. Підготовлено: Іваненко Я. 20.12.19. 00.36

https://www.youtube.com/watch?v=pbyZpCk3tds

Андрій Доманський, відомий телеведучий та актор рекламує крабові палочки «Крабов'є» вже 6 місяців, запевняючи, що палички торгової марки «Водный Мир», виготовлені з м'яса білої риби.

2.2 Апеляція до «добрих почуттів»

Сюжет будується таким чином, щоб товар асоціювався з подіями, що викликають позитивні емоції. Дружба, зустріч із батьками, спорудження нового будинку, здача іспиту та ін.

Приклад 2.2.1. Підготовлено: Іваненко Я.О. 20.12.19. 00.39

https://www.youtube.com/watch?v=v2DLHFEcajE

Спекулюючи на дружніх, теплих стосунках в родині, рекламодавець нав'язує необхідність придбати багато речей, виготовлених виробником даної марки («Фрекен Бок»), завдяки яким, начебто, можна створити таку теплу та приємну атмосферу в родині.

Приклад 2.2.2. Підготовлено:

Опис, коментар, пояснення.

2.3. Назва

Сутність прийому (коротко).

Приклад 2.3.1. Підготовлено:

Опис, коментар, пояснення.

Приклад 2.3.2. Підготовлено:

Опис, коментар, пояснення.