МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КРЕМЕНЧУЦЬКИЙ ЛЬОТНИЙ КОЛЕДЖ

Циклова комісія економіки та управління

ТЕКСТ ЛЕКЦІЙ

навчальної дисципліни «Електронна логістика»
вибіркових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти

Логістика

За темою №8 «Безпека в інформаційних системах»

м. Харків 2021

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.21№ 8

СХВАЛЕНО
Методичною радою
Кременчуцького льотного
коледжу Харківського
національного університету
внутрішніх справ
Протокол від 22.09.21№ 2

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з гуманітарних та соціально-
економічних дисциплін
Протокол від 22.09.21 № 8

Розглянуто на засіданні циклової комісії економіки та управління, протокол від 31.08.2021 № 1

Розробники: старший викладач циклової комісії економіки та управління, к.е.н., спеціаліст вищої категорії, викладач – методист, Харченко М.В.

Рецензенти:

1. Голова циклової комісії економіки та управління КЛК ХНУВС, к.е.н., спеціаліст вищої категорії, старший викладач – методист Цимбалістова О.А.
2. Професор кафедри логістики НАУ, доктор економічних наук, професор, експерт Українського логістичного альянсу (УЛА) Смерічевська С.В.

План лекцій:

1 Безпека підприємства.
2 Інформаційна безпека.
3 Основні заходи інформаційної безпеки.
4 Електронний цифровий підпис.
5 Вітчизняні засоби захисту інформації.

Рекомендована література:

Основна:

1. Валькова Н.В. Електронна логістика: визначення та складові її інструментарію // Моделювання регіональної економіки. Збірник наукових праць.-Івано-Франківськ:Плай, 2013.- №1 (21).-с.119-127
2. Ігнатенко І.В., Пічугіна М.А. Розвиток електронної комерції та фактори впливу / збірника Міжнародної науково-практичної конференції, 2018. – 46 с.
3. Качуровський В. Є. Інформаційна логістика / В. Є. Качуровський // Вісник Національного університету «Львівська політехніка». Серія «Логістика». — 2010. — № 690. — С. 53—59.
4. Скіцько В. І. Електронна логістика як складова сучасного бізнесу / В. І. Скіцько // Бізнес Інформ. – 2014. – № 7. – С. 309-314.
5. Краморенко Н.Р. Особливості розвитку українського сегменту електронної комерції / Краморенко Н.Р. // Інноваційна економіка. – 2011. – № 3. - с. 68-73.
6. Організація та проектування логістичних систем : підручник / За ред. проф. М. П. Денисенка, проф. П. Р. Лековця, проф. Л. І. Михайлової. – К. : Центр навчальної літератури, 2010. – 336 с.
7. Про електронні документи та електронний документообіг. Закон України від 3.09.2015 року N 675-VIII// Відомості Верховної Ради. – 2015, N 36, ст.275 55. Про електронний цифровий підпис. Закон України від 6.10.2016, N 1666- VIII, N 47, ст.800
8. Тардаскіна Т.М. Електронна комерція: Навч. посібник / Т.М. Тардаскіна, Є.М. Стрельчук, Ю.В. Терешко. – Одеса: ОНАЗ ім. О.С. Попова, 2011. – 244 с. Шалева О.І. Електронна комерція: Навч. посібник / О.І. Шалева. — К.:Центр учбової літератури, 2011. — 209 с.
9. Щерба О. Ф. Особливості розвитку електронної торгівлі в Україні / О. Ф. Щерба, Л. Д. Сисюк – 2010. – 103 с.

Допоміжна:

10. Іваницька Т.Є. Методичний підхід до оцінки ефективності управління підприємством на основі логістичних критеріїв / Т.Є. Іваницька // Економіка. Управління. Інновації. – 2013. - №2.
11. Іваницька Т.Є. Методичний підхід до оцінки ефективності управління підприємством на основі логістичних критеріїв / Т.Є. Іваницька // Економіка. Управління. Інновації. – 2013. - №2.
12. Корбутяк В.І. Електронний документообіг та ефективність роботи органів державної влади / В.І. Корбутяк // Науковий вісник Академії муніципального управління. Серія: Управління. – 2013. – Вип. 1. – С. 69-76.
13. О.Хромов Логістика, Видавництво – Бурун Книга, 2012 – 224 с.
14. Осипов В. І. Економіка підприємства : підруч. для студ. вищих навч. закладів / В. І. Осипов. – О. : Маяк, 2010. – 724 с.
15. Паласюк Б. Логістичне управління підприємством: сутність і основні принципи / Б. Паласюк // Галицький економічний вісник. – 2012. - №3(36).
16. Положення про електронні гроші в Україні : Постанова № 481 Правління Національного банку України від 04.11.2010 р.
17. Про електронну комерцію: Закон України № 675-VIII від 3 вересня 2015 р.
18. Пушкар О.І., Віртуальні підприємства та електронний бізнес: конспект лекцій / О.І. Пушкар, Є.М. Грабовський. – Х.:ХНЕУ, 2008. - 47 с.
19. Юдін О. М. Системи електронної комерції: створення, просунення і розвиток :монографія / О. М. Юдін, М. В. Макарова, Р. М. Лавренюк. – Полтава : РВВ ПУЕТ, 2011. – 201 с.

Інформаційні ресурси в Інтернеті

20. China's E-CommerceMarket: The Logistics Challenges: [Електронний ресурс]. – режим доступу http://www.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/chinas-e-commerce-market-thelogistics-challenges/10192
21. Emerging Ecommerce Trendsfor 2012 : [Електронний ресурс]. – режим доступу http://www.zippycart.com/ecommerce-news/3163-merchants-takenote-ecommerce-trends-for 2012.html
22. Logistics and E-commerce: [Електронний ресурс]. – режим доступу http://people.hofstra.edu/geotrans/index.html
23. Ринок e-commerce в Україні URL: http://www.kreditprombank.com/upload/content/512/Ecommerce_Market_in_Ukrain e.pdf
24. Премія E-Awards 2017 назвала кращих гравців українського ринку ecommerce URL: https://interfax.com.ua/news/press-release/415241.html
25. Матеріли сайту Logistic-info URL: http://www.logistike.com/
26. Експерт: обсяг ринку електронної комерції в Україні щомісячно збільшується на 50%: [Електронний ресурс]. – режим доступу http://www.newsru.ua/finance/15may2011/vonline.html
27. Обсяги інтернет-торгівлі в Україні виросли на 32%: [Електронний ресурс].

– режим доступу http://watcher.com.ua/2011/11/24/obsyahy-internet-torhivliv-ukrayini-vyrosly-na-32/
28. Обсяги інтернет-торгівлі в Україні виросли на 32%: [Електронний ресурс]. – режим доступу http://watcher.com.ua/2011/11/24/obsyahy-internet-torhivliv-ukrayini-vyrosly-na-32/ Вільна енциклопедія: [Електронний ресурс]. – режим доступу http://uk.wikipedia.org/
29. Офіційний сайт Асоціації Товарної Нумерації України «ДжіЕс1 Україна» [Електронний ресурс]. – Режим доступу : http://www.gs1ua.org/uk.csp
30. Положення про штрихове кодування та участь у всесвітній системі GS1 // Офіційний сайт Асоціації Товарної Нумерації України «ДжіЕс1 Україна» [Електронний ресурс]. – Режим доступу : http://www.gs1ua.org/files/gs1ua/Polozhennya.pdf

Текст лекції

8.1 Безпека підприємства

Економічна безпека – це складна багатофакторна категорія, яка дозволяє зберігати стійкість до зовнішніх та внутрішніх загроз, характеризує здатність національної економіки до розширеного самовідтворення для задоволення потреб громадян, суспільства і держави на якомусь визначеному рівні.

Економічна безпека – стан економіки, за якого забезпечується досить високе і стійке економічне зростання; ефективне задоволення економічних потреб; контроль держави за рухом і використанням національних ресурсів; захист економічних інтересів країни на національному і міжнародному рівнях.

Економічна безпека поділяється на:
– абсолютну, властиву лише замкнутим детермінованим системам, для яких можлива ліквідація усього спектру загроз;
– відносну, притаманну всім без винятку реальним економічним системам, які, безумовно, є відкритими та залежними від постійного впливу різних перешкод і загроз, що здебільшого має стохастичний характер і об’єктивно не може бути повністю ліквідованими.

Джерела та фактори загроз внутрішній безпеці:
1) невідповідність кваліфікації співробітників обійманій посаді (небезпека, що спричиняє збитки);
2) недостатня кваліфікація працівників (проблема, вирішити яку зобов’язані кадровики);
3) слабка організація системи управління персоналом (немає філософії підприємства);
4) слабка організація системи навчання (відсутня система обліку перспектив розвитку персоналу, що створює соціальну непевність у стабільності свого кар’єрного росту);

5) неефективна система мотивації (немає аналізу потреб кожної особистості й персональної мотивації);
6) помилки в плануванні ресурсів персоналу (найчастіше на просту роботу приймають висококваліфікований персонал);
7) відсутність творчих елементів у роботі;
8) нецільове використання кваліфікованих співробітників;
9) працівники орієнтовані на вирішення внутрішніх тактичних завдань;
10) співробітники не орієнтовані на дотримання інтересів підрозділу (немає цільового управління);
11) відсутність або слабкість корпоративної політики;
12) неякісні перевірки кандидатів під час прийому на роботу.

Джерела та фактори загроз зовнішньої небезпеки:
1) умови мотивації в конкурентів кращі;
2) установка конкурентів на «переманювання»;
3) зовнішній тиск на співробітників;
4) втягування їх у різні види залежності;
5) інфляційні процеси (їх варто враховувати під час розрахунку заробітної плати)

У контексті економічної безпеки логістичних утворень економічна безпека розглядається як поняття, що відображає в інтегрально-комплексному вигляді суб'єктно-об'єктні зв'язки та інші функціональні відношення компонентів економічної системи суб'єктів логістичної діяльності.

Наявні зв'язки і відношення формуються для досягнення цілей логістичної діяльності в умовах мінливого зовнішнього середовища.

Види форм структурування суб'єктів логістичної діяльності:
1. ***Базові:***
- параметричні;
- функціональні;
- мікрологістичні
2. ***Інтеграційні:***
- логістичний канал;
- ланцюг по стачань;
- логістична мережа.

Виходячи з форм структурування, усі суб'єкти логістичної діяльності є організаційними логістичними структурами, що відіграють роль елементів, ланок та підсистем логістичних систем різного рівня.

8.2 Інформаційна безпека

Інформаційна безпека - це стан захищеності систем обробки і зберігання даних,

при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

До основних завдань у сфері захисту інформації (ЗІ) в інформаційно-телекомунікаційних системах у цілому належать:

- керування доступом користувачів до інформаційних ресурсів систем з метою захисту від неправомірного випадкового або навмисного втручання у роботу і несанкціонованого (із перевищенням наданих повноважень) доступу до програмних і апаратних ресурсів як персоналу, так і сторонніх осіб;
- захист даних, що передаються каналами зв'язку;
- захист інформації з обмеженим доступом від витоку;
- захист інформації від спеціальних впливів;
- реєстрація, збереження і надання даних про події, що відбувалися у системі і стосувалися інформаційної безпеки (ІБ);
- контроль роботи користувачів системи адміністраторами та обов'язкове повідомлення адміністратора безпеки про будьякі спроби несанкціонованого доступу до ресурсів системи;
- контроль і підтримка цілісності критичних ресурсів системи захисту і середовища виконання прикладних програм;
- забезпечення функціонування програмно-технічних комплексів з метою захисту інформації від впровадження у роботу потенційно небезпечних програм і засобів подолання системи захисту;
- керування та моніторинг засобів захисту інформації.

Загрози кібербезпеці актуалізуються через чинники:

- невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
- безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструк тури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

- недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Стандарти інформаційної безпеки («Європейські критерії»), що розроблені у країнах Європи (Франція, Німеччина, Нідерланди та Великобританія) розглядають такі завдання інформаційної безпеки:
- захист інформації від несанкціонованого доступу з метою забезпечення конфіденційності;
- забезпечення цілісності інформації за допомогою захисту її від несанкціонованої модифікації або знищення;
- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Напрямки державної інформаційної політики України, що визначені Законом України «Про інформацію»:
- забезпечення доступу кожного до інформації;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
- створення умов для формування в Україні інформаційного суспільства;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
- створення інформаційних систем і мереж інформації, розвиток електронного урядування;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- забезпечення інформаційної безпеки України;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

У Законі України "Про безпеку користувачів телекомунікацій" зазначено, що користувач – це фізична особа, яка користується інформаційною послугою для задоволення своїх споживчих чи ділових потреб, використовуючи кінцеве обладнання, розташоване на території України, але ж як користувач може використовувати ту чи іншу інформацію в Інтернеті для задоволення своїх потреб, якщо його на кожному кроці намагаються обманути?

Гарантія прав споживачів (ЗУ): постачальник інформаційної послуги повинен вживати відповідних технічних та організаційних заходів для гарантування безпеки своїх послуг, захисту інформації, запобігання несанкціонованого доступу до телекомунікацій відповідно до вимог законодавства про захист інформації в автоматизованих системах.

Постачальник несе відповідальність за надання інформаційної послуги, яка містить заборонену до поширення інформацію, відповідно до законодавства.

8.3 Основні заходи інформаційної безпеки

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

У Законі визначено:

- об'єкти захисту в системі та суб'єкти відносин;
- порядок доступу до інформації в системі;
- відносини між володільцем інформації, власником інформаційно-телекомунікаційної системи та користувачами;
- умови обробки та забезпечення захисту інформації в системі;
- повноваження державних органів;
- відповідальність за порушення законодавства, міжнародні договори та прикінцеві положення.

Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмнотехнічні і організаційно-економічні методи.

Правові методи – передбачають розробку комплексу нормативно-правових актів і положень, які регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки.

Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих систем згідно вимогам інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту інформації, контроль за діями персоналу в захищених інформаційних системах.

Програмнотехнічні методи – це сукупність засобів для:

- запобігання витоку інформації;
- виключення можливості несанкціонованого доступу до інформації;
- запобігання впливам, які призводять до знищення, руйнування, спотворення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації; виявлення прикладних пристроїв;

- виключення перехоплення інформації технічними засобами;
- використання криптографічних засобів захисту інформації при передачі по каналах зв’язку.

До основних заходів безпеки в електронному бізнесі відносяться:
- забезпечення захисту інформаційних і телекомунікаційних систем від несанкціонованого доступу, обмеження доступу співробітників, контроль і облік доступу, розмежування прав доступу користувачів до інформаційної системи відповідно до їх посадовими обов'язками;
- забезпечення захисту ЕДО за допомогою ЕЦП або іншого аналога власноручного підпису, застосуванням цифрових сертифікатів;
- забезпечення криптографічного захисту при передачі інформації в інформаційних системах;
- встановлення вимог щодо інформаційної безпеки інформаційних об'єктів, контроль їх виконання.

Захист інформації від несанкціонованого використання для великих торгових підприємств є більш трудомісткою з огляду на те, що вони мають розгалужену територіальну структуру.

Для захисту корпоративної інфраструктури використовуються методи аутентифікації і ідентифікації користувачів і пристроїв, шифрування даних, створення захисних бар'єрів, що оберігають від проникнення в корпоративну мережу ззовні.

До засобів інформаційної безпеки, що використовуються компаніями, відносяться:
- ТББ-шифрування,
- аутентифікація (в тому числі і двухфакторная, 2БА),
- ідентифікація,
- авторизація,
- перевірка цілісності і призначені для захисту законних користувачів інформаційної системи від неправомірних дій зловмисників.

Об'єктами і суб'єктами ідентифікації і аутентифікації можуть бути люди (абоненти кінцевих терміналів, оператори), технічні засоби, носії інформації, документи та ін.

Ідентифікація - це присвоєння будь-якого об'єкта чи суб'єкту унікального імені (Login, LoginName, UserName) або образу. *З цього імені здійснюється ототожнення істинного користувача при зверненні користувача до певного сервісу.*

Авторизація - операція перевірки дозволів та прав, наданих користувачеві. В ЕК в процесі авторизації може встановлюватися кредитоспроможність клієнта. *До подальших операцій після авторизації клієнт допускається лише при*

наявності у нього необхідної для покупки товару або послуги суми грошей. Таку авторизацію здійснюють електронні платіжні системи.

Стандарт FIPS 113 COMPUTER DATA AUTHENTICATION призначений для контролю цілісності інформації, що передається, яка проводиться засобами криптографічного аутентифікації.

Аутентифікація - це підтвердження (встановлення) дійсності об'єкта або суб'єкта взаємодії в інформаційній мережі по висунутій ідентифікатором. Ідентифікатор - ім'я, під яким зареєстрований користувач в перевіряє його інформаційній системі. *У процесі аутентифікації встановлюється правомірність користувача з'єднуватися з сервером, проводиться перевірка справжності абонента. Встановлюється, що повідомлення належить законному абоненту, а не зловмисникові. Для аутентифікації використовуються як програмні, так і апаратні засоби. У компанії може бути кілька інформаційних систем і джерел інформації, які потребують аутентифікації.* **Інформаційні системи:**

- корпоративний портал;
- електронна пошта;
- CRM-система;
- віддалений VPN-доступ;
- локальна мережа Wi-Fi і ін.

До основних видів аутентифікації відносяться:

1) ***одностороння і взаємна.*** *Проведена з використанням аутентифікації перевірка або підтвердження автентичності може виконуватися однією стороною або здійснюватися всіма взаємодіючими сторонами. Як приклад наведемо двосторонню аутентифікацію, здійснювану при здійсненні платежів за поставлені товари в підсистемі CyberCheck платіжної системи CyberPlat. Фірма-покупець (далі - Покупець) заходить на сайт фірми-продавця (далі - Продавець), формує кошик необхідних їй товарів. Продавець виставляє рахунок, підписує його своїм ЕЦП та надсилає його Покупцеві. Покупець підписує рахунок своєї ЕЦП, після чого рахунок називається чеком. чек, підписаний ЕЦП двох сторін, відправляється в банк для оплати. Ідентифікаторами в даному випадку є ЕЦП Продавця і Покупця;*

2) ***проста і сувора***. У ГОСТ Р ISO / IEC 9594-8-98 розглядаються проста і сувора аутентифікація. При простій аутентифікації в якості ідентифікатора використовується пароль.

При суворої аутентифікації ідентифікатор створюється з використанням криптографічних методів.

Проста аутентифікація реалізується в результаті виконання наступних кроків:

- суб'єкт вводить особистий ідентифікатор (логін) і пароль в інформаційну систему для отримання доступу до неї;
- введені дані надходять на сервер аутентифікації, де порівнюються з зразковими даними суб'єкта, введеними раніше;
- суб'єкт отримує доступ до інформаційної системи при збігу введених даних з зразковими даними. *При розбіжності даних йому пропонується ввести дані заново*.

8.4 Електронний цифровий підпис

Регулювання: **ЗУ «Про електронний цифровий підпис», 2003 р.**
Відповідно до Закону, якщо створюються ідентичні за документарною інформацією та реквізитами електронний документ і документ на папері, кожен з документів є оригіналом та має однакову юридичну силу.

Допустимість електронного документа як доказу не може заперечуватися лише на підставі того, що він має електронну форму.

Типовий закон UNCITRAL про електронні підписи від 2001 р.
Як вбачається з його преамбули, закон застосовується в тих випадках, коли електронні підписи використовуються в контексті торгівельної діяльності та не має переважної сили по відношенню до будь-яких норм права, призначених для захисту споживачів.

Закон UNCITRAL про електронні підписи від 2001 р. встановлює:
- режим для технологій створення електронних підписів;
- положення про дотримання вимоги щодо наявності підпису;
- поведінку підписанта;
- поведінку постачальника сертифікаційних послуг;
- процедуру визнання іноземних сертифікатів і електронних підписів.

Електронний підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

Електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додасться до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

Засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій - призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

Особистий ключ - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;
відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

Засвідчення чинності відкритого ключа - процедура формування сертифіката відкритого ключа;

Сертифікат відкритого ключа - документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу.
Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача.

8.5 Вітчизняні засоби захисту інформації

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи.

Метод передбачає певну послідовність дій на підставі конкретного плану.

Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи описи і класифікації.

Для здійснення ефективного захисту системи управління слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження при чинних зв'язків.

За допомогою даних методів виявляються:
- причинні зв'язки між загрозами та небезпеками;

- здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації.

Методи причинних зв'язків:
- метод схожості,
- метод розбіжності,
- метод сполучення схожості і розбіжності,
- метод супроводжувальних змін, метод залишків.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту.
В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту.

Загрози у сфери інформаційної безпеки:
1) фізичний;
2) програмно-технічний;
3) управлінський;
4) технологічний;
5) рівень користувача;
6) мережевий;
7) процедурний.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Типи методів забезпечення інформаційної безпеки:

1) одноріневі методи будуються на підставі одного принципу управління інформаційною безпекою;
2) багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;
3) комплексні методи — багаторівневі технології, які об'єднані у єдину систему координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;
4) інтегровані високоінтелектуальні методи — багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами.

Стадії:

- прийняття рішення по визначенню області та контексту інформаційної загрози і складу учасників процесу протидії;
- ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності;
- забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних ланках системи управління НБ;
- виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.