Міністерство освіти і науки України
Національний університет водного господарства та природокористування

Кафедра державного управління, документознавства та інформаційної діяльності

06-14-208М

МЕТОДИЧНІ ВКАЗІВКИ

до практичних робіт та виконання самостійної роботи
з навчальної дисципліни
«Інформаційна безпека»
для здобувачів вищої освіти першого (бакалаврського) рівня
за освітньо-професійною програмою
«Управління інформаційними комунікаціями»
спеціальності 029 «Інформаційна, бібліотечна та архівна справа»
денної форми навчання

Рекомендовано
науково-методичною радою
з якості ННІЕМ
Протокол № 2 від 19.10 2021 р.

Рівне – 2021

Методичні вказівки до практичних робіт та виконання самостійної роботи з навчальної дисципліни «Інформаційна безпека» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Управління інформаційними комунікаціями» спеціальності 029 «Інформаційна, бібліотечна та архівна справа» денної форми навчання [Електронне видання] / Маланчук Л. О. – Рівне : НУВГП, 2021. – 51 с.

Укладач: Маланчук Л. О., к.е.н., доцент кафедри державного управління, документознавства та інформаційної діяльності.

Відповідальний за випуск: Тихончук Л. Х., д.держ.упр., доцент, в.о. завідувача кафедри державного управління, документознавства та інформаційної діяльності.

Керівник групи забезпечення
спеціальності
к.і.н,доцент Цецик Я. П.

ЗМІСТ

1. Загальні положення вивчення навчальної дисципліни

Навчальна дисципліна «Інформаційна безпека» призначена для вивчення здобувачами вищої освіти першого (бакалаврського) рівня за спеціальністю 029 «Інформаціна, бібліотечна та архівна справа» та є однією з професійно орієнтованих дисциплін, що дозволяє набути компетентності в сфері інформаційної безпеки.

Завданнями вивчення навчальної дисципліни є: ознайомлення із загальнодержавними програмами та напрямками інформатизації державного управління; вивчення основних процесів інформаційних технологій забезпечення управлінської діяльності; визначення критеріїв вибору та застосування інформаційно-комунікаційних мереж і їх складових у забезпеченні управлінської та адміністративної діяльності; вивчення вимог щодо сучасної постановки завдань захисту інформації; визначення стратегії захисту інформації; ознайомлення із класифікацію і змістом загроз інформації; методи визначення вимог до захисту інформації; вивчення засобів і систем захисту інформації

Метою викладання навчальної дисципліни є забезпечення достатнього рівня теоретичних знань про сутність інформаційної безпеки, сформувати у студентів систему знань по інформаційній безпеці і захисту інформації, а також ознайомити студентів із загальними принципами системи захисту інформації, концептуальною моделлю інформаційної безпеки, видами забезпечення системи захисту інформації: правовим, організаційним, апаратним, інформаційним, програмним, математичним, лінгвістичним, нормативно-методичним та формування практичних навичок захисту інформації у процесі здійснення публічної управлінської діяльності та адміністрування. Після вивчення даної дисципліни здобувачі вищої освіти повинні:

набути таких компетентностей:

1. Здатність до абстрактного мислення, аналізу та синтезу.
2. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).
3. Здатність проектувати та створювати документно-інформаційні ресурси, продукти та послуги.
4. Здатність здійснювати відбір, аналіз, оцінку, систематизацію, моніторинг, організацію, зберігання, розповсюдження та надання в користування інформації та знань у будь-яких форматах.
5. Здатність використовувати сучасні прикладні комп’ютерні технології, програмне забезпечення, мережеві та мобільні технології для вирішення професійних завдань.
6. Здатність адмініструвати соціальні мережі, електронні бібліотеки та архіви.
7. Здатність здійснювати захист інформації на різних типах носіїв

мати результати навчання:

1. Знати і розуміти наукові засади організації, модернізації та впровадження новітніх технологій в інформаційній, бібліотечній та архівній діяльності.
2. Застосовувати у професійній діяльності технології інформаційного менеджменту, створення і підтримки функціонування електронних бібліотек та архівів, методологію вивчення та задоволення культурних та інформаційних потреб користувачів
3. Оцінювати можливості застосування новітніх інформаційно-комп’ютерних

та комунікаційних технологій для вдосконалення практик виробництва інформаційних продуктів і послуг.

4. Застосовувати сучасні методики і технології автоматизованого опрацювання інформації, формування та використання електронних інформаційних ресурсів та сервісів
5. Дотримуватися і реалізовувати основні засади охорони праці та безпеки життєдіяльності.
6. Кваліфіковано захищати й використовувати інформацію в умовах загроз та інформаційних протистоянь.

Предметом навчальної дисципліни є методика та основні засади захисту інформації при організації управлінсько-адміністративної діяльності в організаціях та установах.

2. Поради з планування і організації вивчення навчальної дисципліни

Самостійна робота здобувача є одним із важливих засобів оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять. Зміст самостійної роботи при вивченні дисципліни «Електронний документообіг та електронне урядування» визначається навчальною програмою дисципліни, завданнями та вказівками викладача, даними методичними вказівками. Головною метою самостійної роботи є закріплення, розширення та поглиблення набутих у процесі аудиторної роботи знань, вмінь та навичок, а також самостійне вивчення та засвоєння нового матеріалу під керівництвом викладача. Питання, що виникають у здобувачів стосовно виконання запланованих завдань, вирішуються на консультаціях, які проводяться згідно графіку, затвердженого кафедрою державного управління, документознавства та інформаційної діяльності.

Самостійна робота здобувачів під час вивчення навчальної дисципліни «Інформаційна безпека» включає такі форми:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем і питань, які передбачені для самостійного опрацювання;
- підготовка до практичних занять;
- систематизація вивченого матеріалу дисципліни перед проведенням модульних контролів;
- підготовка наукової статті (есе) за програмою дисципліни;
- підготовка доповідей та участь в наукових студентських конференціях, круглих столах, тощо.

Всі завдання самостійної роботи здобувачів поділяються на обов'язкові та вибіркові, виконуються у встановлені терміни, з відповідною максимальною оцінкою та передбачають певні форми звітності щодо їх виконання. Обов'язкові завдання виконуються кожним без винятку здобувачем у процесі вивчення навчальної дисципліни, вибіркові завдання є альтернативними.

Після виконання обов'язкових та вибіркових завдань у встановлені терміни студент звітує викладачеві, а набрані ним бали враховуються як кількість балів за поточну успішність в навчальній роботі.

Оцінювання результатів поточної роботи (завдань, що виконуються на практичних, індивідуальних заняттях та консультаціях, результати самостійної роботи студентів) проводиться за такими критеріями (у відсотках від кількості балів, виділених на завдання із

заокругленням до цілого числа):

а) 100 % - завдання виконано правильно, вчасно і без зауважень;

а) 80 % - завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

а) 60 % - завдання виконане повністю, але містить суттєві помилки у розрахунках або в методиці;

б) 40 % - завдання виконане частково та містить суттєві помилки методичного або розрахункового характеру;

б) 0 % - завдання не виконане.

В процесі вивчення здобувачами дисципліни «Електронний документообіг та електронне урядування» передбачено наступні види роботи викладачів зі здобувачами:

- індивідуальні консультації за графіком, затвердженим кафедрою державного управління, документознавства та інформаційної діяльності;
- перевірка виконання індивідуальних завдань поточного контролю та модульних контрольних робіт;
- індивідуальні заняття зі здобувачами з метою підвищення рівня їхньої підготовки та розвитку індивідуальних здібностей, результатом яких може бути підготовка наукових доповідей, статей.

Контроль самостійної роботи здобувачів здійснюється на практичних та індивідуальних заняттях у формі поточного контролю, модульних контрольних робіт та перевірки якості виконання домашніх завдань. У табл. 1 наведено завдання для самостійного опрацювання.

Таблиця 1

Перелік питань для підготовки доповіді (інформаційного повідомлення, презентації)

№ з/п	Назва теми
1.	Поняття та основні задачі інформаційної безпеки
2.	Загрози інформаційної безпеки
3.	Системи забезпечення інформаційної безпеки
4.	Основні сервіси безепеки
5.	Особливості сучасних інформаційних систем з погляду безпеки
6.	Фізичні засоби захисту
7.	Інформаційні ресурси
8.	Інформаційна безпека в електронному урядуванні
9.	Інформаційні виборчі технології
10.	Огляд міжнародних стандартів у галузі інформаційна безпека
11.	Основні положення теорії захисту інформації 1
12.	Сутність та види атак на комп’ютерну мережу
13.	Реалізація системи захисту інформації в комп’ютерних системах і мережах
14.	Інформаційне та правове забезпечення електронних видань і цифрової передачі даних в Україні

15.	Міжнародна інформаційна безпека
16.	Технологія реалізації атак на комп'ютерну систему та мережу
17.	Законодавча база в галузі захисту інформації

Інформаційна безпека України є органічною складовою національної, відтак її розгляд є необхідним для формування базових знань та уявлень про національну безпеку.

Актуальність розгляду даної теми обумовлена цілою низкою чинників:

- нині головним стратегічним національним ресурсом, основою економічної та оборонної могутності держави стає інформація та інформаційні технології;
- інформація у сучасному світі є таким атрибутом, від якого у визначальному плані залежить ефективність життєдіяльності сучасного суспільства;
- інформаційні технології принципово змінили обсяг і важливість інформації, яка обертається в технічних засобах її збереження, обробки та передачі;
- загальна комп'ютеризація основних сфер діяльності призвела до появи широкого спектру внутрішніх і зовнішніх загроз, нетрадиційних каналів втрати інформації і несанкціонованого доступу до неї;
- масове оснащення державних установ, підприємств, організацій і приватних осіб засобами обчислювальної техніки і включення їх до світових інформаційних просторів містить у собі реальну загрозу створення розгалужених систем регулярного несанкціонованого контролю за інформаційними процесами і ресурсами, навмисного втручання в них;
- реальністю сьогодення стало застосування інформаційної зброї і ведення інформаційних війн;
- недосконаліть правового регулювання суспільних відносин
- у сфері інформаційної безпеки призводить до серйозних негативних наслідків, які ускладнюють підтримання необхідного балансу інтересів особи, суспільства та держави, формування конкурентоспроможних місцевих інформаційних агентств і засобів масової інформації;
- недобросовісне використання інформаційного простору усередині держави призводить до зниження рівня внутрішньої інформаційної безпеки України, прямим наслідком чого є дестабілізація соціально-політичної обстановки, проведення акцій опору прийняттю тих чи інших державних рішень;
- конституційні права громадян на недоторканність приватного життя, особистої та сімейної таємниці, таємниці листування не мають достатнього організаційно-правового і технічного забезпечення;
- погіршується ситуація із забезпеченням збереження державної таємниці, недостатньо розвинені механізми забезпечення службової та комерційної таємниці;
- суттєва шкода завдана кадровому потенціалу колективів тих підприємств, які діють у сфері створення засобів інформатизації;
- відставання вітчизняних інформаційних технологій змушує при створенні інформаційних систем закуповувати імпортну техніку І залучати іноземні фірми, через

що підвищується імовірність несанкціонованого доступу до інформації, що обробляється, зростає залежність від іноземних виробників комп'ютерної і телекомунікаційної техніки, програмного забезпечення.

Відтак процес інформатизації суспільства розвивається стрімко і почасти непередбачено. Інформатизація призводить до створення єдиного інформаційного простору, в межах якого відбувається накопичення, обробка, зберігання, обмін інформацією між суб'єктами цього простору — окремими особами, організаціями, державами.

Нормальна життєдіяльність суспільства визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища, а також рівнем і станом нормативно-правового забезпечення даних процесів. Інформаційне законодавство спрямовано на закріплення державної інформаційної політики, яка передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері, нормального розвитку інформаційних технологій і засобів захисту інформації, виключення монополізму в даній області, запобігання розроблення інформаційно деструктивних технологій впливу на антропогенну популяцію, захист авторських і суміжних прав тощо.

Виробництво й управління, оборона і зв'язок, транспорт і енергетика, банківська справа, фінанси, наука й освіта, медицина, екологія — все більше залежать від інтенсивності інформаційного обміну, повноти, своєчасності та достовірності інформації.

Поява й активізації загроз в інформаційній сфері, передусім загроз від ведення інформаційних війн, суттєво підвищує роль і значення інформаційної безпеки в системі національної безпеки України і обумовлює розширення її змісту. Віра та контроль над національними інформаційними комунікаціями у XXI столітті може призвести до втрати національної незалежності. Майбутні війни — війни без застосування прямого насильства, засобами якого є непрямі дії, одним з методів яких можуть бути інформаційні війни.

Особливо слід відмітити важливість широкого застосування загальноосвітніх курсів інформаційної безпеки при підготовці кадрів різної професійної спрямованості з урахуванням перспектив розвитку інформаційної цивілізації.

Поняття та зміст інформаційної безпеки

Характерною ознакою сучасного етапу економічного та науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх якнайширше використання як у повсякденному житті, так і управлінні державою. Інформація і інформаційні технології все більше визначають розвиток суспільства та слугують новими джерелами національної могутності. Становлення інформаційного суспільства радикально змінює політичну, екологічну та соціальну сфери життєдіяльності людства. У цих умовах формування інформаційного суспільства змінює предмет праці на інформацію і знання. У свою чергу основою глобалізації стають інтеграція інформаційних систем різних держав до єдиної загальносвітової інформаційної системи, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних тенет, інтенсивне впровадження

нових інформаційних технологій в усі галузі суспільного життя, включаючи і державне управління.

Глобальний процес інформатизації суспільства охопив практично всі країни світу і нині є стрижнем науково-технічного і соціально-економічного розвитку.

Інформатизація становить собою організаційний соціально-економічний і науково-технічний процес створення оптимальних умов для всебічного задоволення інформаційних потреб і реалізації прав громадян суспільства, органів державної влади й управління на основі формування і використання інформаційних ресурсів і використання інформаційних систем, мереж, ресурсів і інформаційних технологій із використанням обчислювальної і комунікаційної техніки.

Основними завданнями інформатизації є:

- • всебічне інформаційне забезпечення потреб суб'єктів інформаційних відносин;
- • створення єдиного безпечного інформаційного простору;
- • створення, впровадження і використання інформаційних систем, інформаційних технологій і інформаційних продуктів загального значення;
- • підготовка кадрів, підвищення їх кваліфікації у сфері інформатизації.

Осягнення сутності змісту поняття "інформаційна безпека" є важливим завданнями наукового аналізу. Будь-яке вчення лише тоді досягає зрілості і досконалості, коли розкриває сутність досліджуваних явищ, має можливість передбачати майбутні зміни не лише у сфері явищ, а й у сфері сутностей. Пізнання сутності інформаційної безпеки можливо лише на основі абстрактного мислення, створення теорії досліджуваного предмета, усвідомлення внутрішнього змісту, виявлення характерних ознак, розкриття сутнісних характеристик поняття, що вивчається.

В історичному процесі складається структура предмета, тобто єдність внутрішнього змісту і зовнішніх проявів, співпадаючих і неспівпадаючих суперечливих сутностей. Сутність — сукупність глибинних зв'язків, відносин і внутрішніх законів, які визначають основні риси і тенденції розвитку системи. Сутність може вважатися пізнаною, коли відомі причини виникнення і джерела розвитку розглядуваного об'єкта, шляхи його формування або технічного репродукування, якщо в теорії або на практиці створена його достовірна модель. Одна й та сама сутність може мати множину різних явищ.

Сутність проявляється і осягається в дефініції* яке виражає родове оняття. Таким щодо інформаційної безпеки е поняття безпеки, яке характеризує певний процес управління загрозами та небезпеками. Відповідно видове поняття "інформаційна безпека" означає процес управління загрозами та небезпеками в інформаційній сфері.

Саме тому інформаційна безпека е невід'ємною частиною загальної безпеки, чи то національної, чи то регіональної, чи то міжнародної. Аналіз інформаційної безпеки передбачає розгляд сукупності таких об'єктивних чинників:

- потреб громадян, суспільства і держави і світового співтовариства;
- уразливість індивідів, суспільства і держави від цифрових технологій;
- наявність широкого кола загроз і небезпек, якими має управляти система забезпечення інформаційної безпеки.

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття "інформаційна безпека" розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах.

Так, визначення інформаційної безпеки було дано у Федеральному Законі Росії "Про участь у міжнародному інформаційному обміні". У даному законі інформаційна безпека розглядалася як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій і держави. Ця трактовка виходить з того, що захист інформації та інформаційної інфраструктури становить содою зміст інформаційної безпеки. При цьому наголос робиться на технічний бік проблеми.

Дещо інше визначення інформаційної безпеки міститься у Доктрині інформаційної безпеки Російської Федерації, де вона визначається як стан захищеності її національних інтересів у інформаційній сфері, які визначаються сукупністю збалансованих інтересів особи суспільства і держави. З цього визначення випливає, що зміст поняття безпеки базується на інтересах суб'єктів суспільних відносин в інформаційній сфері, від збалансованості яких залежить рівень загроз.

Слід зазначити, що у науковій літературі поки бракує єдиного консолідованого погляду на зміст поняття "інформаційна безпека". Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. Відтак постає необхідність в угрупуванні напрямів визначення аналізованого поняття.

Так, наприклад, представник першого напряму за нашою умовною класифікацією, Ю.А. Фісун, який працює в Академії управління МВС РФ характеризує інформаційну безпеку як "стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх

інформаційних загроз". Такої ж позиції притримуються і розробники концепції інформаційної безпеки центру Разумкова, а також деякі українські дослідники, які вважають за необхідне визначати інформаційну безпеку як стан захищеності. Так наприклад, Гасеський В.К., Авраменко ВА. визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації, у той час як О.Г. Додонов визначає інформаційну безпеку як стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави.

Аналогічного погляду дотримується і інший російський дослідник /. Панарін, роблячи більший акцент на ролі політичної еліти, яка може протистояти інформаційному впливу. На його думку, інформаційна безпека — стан інформаційного середовища суспільства і політичної еліти, який забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства.

Дещо в іншому ракурсі трактує інформаційну безпеку АА. Тер-Акопов, який репрезентує позицію другого напряму. Під інформаційною безпекою він розуміє стан захищеності інформації, яка забезпечує життєво важливі інтереси людини. У рамках даного напряму існує визначення інформаційної безпеки як стану, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів і установ, при яких забезпечується збереження їх якісної з об'єктивними обумовленими інноваціями в ній, і вільне, відповідне власній природі і її функціонування. Ряд представників цього напряму розглядають інформаційну безпеку як стан, який характеризується відсутністю небезпеки, тобто чинників і умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища. Прибічники такого підходу розглядають інформаційну безпеку як стан і процес захищеності особи, суспільства, держави від реальних або потенційних загроз. Водночас, на нашу думку, розглядати безпеку лише як стан є не зовсім точним, і не відображає динамізму як самої безпеки, так і тої системи, для якої безпека виступає як функція її подальшого розвитку та існування.

Поняття процес відрізняється від поняття стан. Поняття процес означає послідовність станів, пов'язаність стадій їх зміни і розвитку, тобто на відміну від поняття "стан", поняття "процес" акцентує увагу на моменті спрямованості в зміні об'єкта, цілепокладанні, тоді як "стан" відображає лише один момент, певну мить безпеки, а отже не вичерпує її повністю.

Представник третього напрями В.І. Ярочкін визначає безпеку як "стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек і загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства з виявлення (вивчення), попередження, послаблення, ліквідації і відбиття небезпек і загроз, здатних загубити їх, лишити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку". Застосування діяльнісного підходу, ва наш погляд, є більш адекватним при описуванні інформаційної безпеки, і ми в певній мірі можемо підтримати дане визначення у загальному плані, однак не погодитись із деталізацією напрямів діяльності, які з часом змінюватимуться, а отже закладатимуть потенціал нестійкості як до самого визначення, так і до функціонування відповідних суб'єктів.

М.П. Хрипков вважає, що діяльність по забезпеченню особи, суспільства і держави виникає в ході вирішення суперечності між такою об'єктивною реальністю, як небезпека, і потребою розумної сутності, соціального індивіда, соціальної групи попередити ЇЇ можливі шкідливі наслідки. Водночас за даного випадку функціонування системи забезпечення інформаційної безпеки зводиться лише до реагування, тоді як превенція лишається поза увагою.

Саме тому, на наше переконання, інформаційна безпека становить собою діяльність органів державного управління. Звідси витікає важливий висновок, що слід діяти активно,

здійснюючи вплив на джерела інформаційної небезпеки. При цьому щодо змісту інформаційної безпеки доцільно використовувати не поняття "інтереси", а більш фундаментальне поняття "цінності", через те, що у цінностях знаходять вираз інтереси суб'єктів суспільних відносин, зіткнення яких породжує загрози.

Наступний погляд передбачає, що у самому загальному вигляді під інформаційною безпекою можна розуміти здатність суб'єкта зберігати свої системостворюючі властивості, основні характеристики при патогенних дезорганізуючих, деструктивних впливах на кіберпростір, інформаційно-комунікаційні технології.

На думку прибічників цього погляду, безпека і забезпечення безпеки становлять собою різні поняття, через те, що безпека виражає характеристику стану соціальної спільноти, тоді як забезпечення безпеки — діяльнісну характеристику, тобто діяльність органів державної влади і управління з підтримання безпеки. У цьому плані безпека усвідомлюється як основа цілепокладання політики, а забезпечення безпеки — як діяльність з досягнення безпечного стану суспільства або соціальної групи. Цієї ж думки дотримується і автор.

Цікавою є думка відомого українського дослідника проблем інформаційної безпеки РЛ. Калюжного, який вважає, що інформаційна безпека — вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації.

У цілому ж інформаційна безпека покликана забезпечити реалізацію національних інтересів за допомогою усього арсеналу засобів, що є в її розпорядженні. У цьому сенсі ми вважаємо, що найвищий сенс політики інформаційної безпеки — вільний розвиток і процвітання суспільства.

Отже, інформаційна безпека являє собою одне з найважливіших понять у науці і різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття "інформаційна безпека" надає можливість зауважити про недоцільність суворого обрання тієї чи іншої позиції. Наведеш вище погляди, а вірніше підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему більш комплексно і системно, додати знань про цей багатогранний феномен. Більш того, на наше переконання, найбільш прийнятним є інтегральний підхід, за якого інформаційна безпека визначатиметься за допомогою окреслення найбільш важливих її сутнісних ознак з урахуванням постійної динаміки інформаційних систем.

Такий підхід надав можливість дійти висновку, що інформаційна безпека не може розглядатися лише як окремий стан. Безперечно, що це є і властивістю, атрибутом інформаційного суспільства, діяльністю і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері. Інформаційна безпека має враховувати майбутнє, а отже, вона не є станом, а становить собою процес. Таким чином, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан,

властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків.

Також наголосимо, що не підтримуємо позицій тих дослідників, які зводять інформаційну безпеку лише до захисту інформації. Інформаційна безпека за своєї суттю є більш широким поняттям. Отже, інформаційна безпека — багатогранна область діяльності, в якій успіх може принести лише системно-комплексний підхід.

Дослідження сутності інформаційної безпеки має враховувати той факт, що сутність є внутрішнім змістом предмету, який знаходить вираз у стійкій єдності усіх багатоманітних і суперечливих формах буття.

Базовою характеристикою інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави.

Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних затрат.

Отже, можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур в рамках міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають дане утворення. В якості останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управління.

Значимість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних і пріоритетних завдань політики національної безпеки.

Як нами вже зазначалося, національні інтереси в інформаційній сфері є похідними від національних цінностей. Отже, інтереси інформаційної безпеки витікають із таких цінностей, як права людини, свобода, економічне процвітання. Саме тому головним інтересом для України є її виживання як вільної незалежної нації при збереженні фундаментальних цінностей і інститутів безпеки.

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування. Відтак інформаційна безпека може описуватися за допомогою терміну "гомеостазис".

До характеристик, за допомогою яких можна описати дану систему, належать:

- доступність — можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб'єктом виконавчої влади;
- цілісність — актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;
- конфіденційність — захист від несанкціонованого ознайомлення.

Сутність і зміст інформаційної безпеки проявляються по-особливому на кожному з рівнів державного управління, зокрема на:

- стратегічному — Кабінет Міністрів України;
- тактичному — центральні органи виконавчої влади;
- оперативному — місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації.

Таким чином можна говорити і про прояви інформаційної безпеки у самому процесі її забезпечення, таким чином можна виділити наступні рівні:

- нормативно-правововий — закони, нормативно-правові акти тощо;
- адміністративний — дії загального характеру, які вживаються органами державного управління;
- процедурний — конкретні процедури забезпечення інформаційної безпеки;
- програмно-технічний — конкретні технічні заходи забезпечення інформаційної безпеки.

Для розкриття сутності та змісту інформаційної безпеки важливим є зв'язок останньої із політикою держави. Складовою частиною політики держави як регулятора суспільних відносин відповідно до гуманістичних начал є обов'язок забезпечення інформаційної безпеки особи, суспільства та держави.

Інформаційна безпека як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. Водночас, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій безпосередній вираз вплив держави, яка за допомогою системи методів виражає загальні цінності у сфері інформаційної безпеки.

Категорійно-понятійна система інформаційної безпеки

Інформаційна безпека — складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України; неухильне дотримання конституційного права громадян на свободу слова

доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Інформаційні відносини — відносини, які виникають у всіх сферах життя і діяльності людини, суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Інформаційний суверенітет — здатність держави контролювати і регулювати потоки інформації поза межами держави з метою додержання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційний простір (національний): 1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави; 2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

Інформаційна інфраструктура: сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництво інформаційних технологій, сервісного обслуговування інфраструктури і системи підготовки кадрів.

Інформаційна система; організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

Інформаційні ресурси: 1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо); 2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави у певній сфері життя чи діяльності.

Інформаційні технологи: 1) цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування; 2) цілеспрямовано організована сукупність інформаційних процесів для створення і використання інформаційних продуктів або надання інформаційних послуг; 3) технологічний процес, предметом перероблення й результатом якого е інформація; 4) процес матеріалізації знань у продукцію і послуги за

допомогою комп'ютерно-телекомунікаційних систем; 5) система методів і способів використання комп'ютерної техніки та систем зв'язку для створення, пошуку, одержання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформаційних продуктів.

Інформаційне середовище: усталене поєднання окремих суб'єктів національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, що взаємодіють в інформаційних процесах.

Інформаційний ринок: система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг

Інформаційний продукт (продукція): 1) документована інформація, яка підготовлена і призначена для задоволення потреб користувачів; 2) документована інформація, яку підготовлено відповідно до потреб користувачів і яка призначена чи застосовується для задоволення потреб користувачів; 3) створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

Інформаційне забезпечення: підтримка засобами систем баз даних і баз знань процесів виробництва, торгівлі, керування, навчання, наукових досліджень та будь-якої іншої діяльності у всіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

Інформаційне поле: 1) сукупність енергетичних субстанцій окремих об'єктів, які є елементами інформаційного поля Землі та Всесвіту; 2) просторово-часові вібрації (інформаційно-розпорядницькі структури), що містять відомості про минуле, сьогодення і майбутнє Всесвіту.

Інформаційне суспільство: 1) суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її вищої форми — знань; 2) суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

Інформатизація: 1) сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки; 2) діяльність, спрямована на створення та широкомасштабне використання в усіх сферах життя суспільства інформаційних технологій.

Інформатика: наукова діяльність, що вивчає інформаційні структури та процеси збирання (набуття, придбання), відображення, реєстрації, накопичення, збереження і поширення (розповсюдження, реалізацію) інформації за допомогою ЕОМ.

Інформаціологія: новітня загальна фундаментальна наука про інформаційні природні процеси матеріалізації та дематеріалізації в мікро- й макроструктурах Всесвіту, що самоорганізуються.

Інформація: 1) документовані або публічно проголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі; 2) відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства, та навколишньому природному середовищі, незалежно від форми їх представленнями) будь-які знання про предмети, факти, поняття і т. ін. проблемної сфери, якими обмінюються користувачі системи оброблення даних.

Інформаційна війна: процес боротьби між суб'єктами із застосуванням інформаційної зброї.

Інформаційна зброя: засоби, які дозволяють вчинювати замислені дії із повідомленнями, що передаються, обробляються, створюються, знищуються і сприймаються.

Інформаційна загроза: вхідні дані, початково призначені для активізації в інформаційній системі алгоритмів, що відповідають за звичайний режим функціонування.

Сугестія: прихований інформаційний вплив на інформаційну систему, що самонавчається.

Сугестивний вплив: вплив з формування у інформаційної системи, що самонавчається, прихованих від неї самої цілей.

Зважаючи на той факт, що будова системи забезпечення внутрішньої інформаційної безпеки є неможливою поза контекстом загроз та небезпек, наступним елементом для розгляду і будуть загрози інформаційній безпеці, що в сукупності дозволить окреслити напрями функціонування системи забезпечення інформаційної безпеки.

Загрози інформаційної безпеки

Загроза інформаційної безпеки — сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки.

Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам.

Під загрозою інтересів суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке з допомогою впливу на інформацію або інші

компоненти інформаційної системи, може прямо або опосередковано призвести до заподіяння шкоди даним того чи іншого суб'єкта

Загрози інформаційної безпеки можуть бути класифіковані за різними ознаками:

- За аспектом інформаційної безпеки, на який спрямовані загрози:
  - *Загрози конфіденційності* (неправомірний доступ до інформації). Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в комп'ютерній системі або передається від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози можуть виникати внаслідок «людського фактора» (наприклад, випадкове делегування тому або іншому користувачеві привілеїв іншого користувача), збоїв роботи програмних та апаратних засобів. До інформації обмеженого доступу належить державна таємниця (комерційна таємниця, персональні дані, професійні види таємниці: лікарська, адвокатська, банківська, службова, нотаріальна таємниця страхування, слідства й судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця), відомості про сутність винаходу, корисної моделі або промислового зразка до офіційної публікації (ноу-хау) та ін).
  - *Загрози цілісності* (неправомірна зміна даних). Загрози порушення цілісності — це загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними чинниками — від умисних дій персоналу до виходу з ладу обладнання.
  - *Загрози доступності* (здійснення дій, які унеможливлюють чи ускладнюють доступ до ресурсів інформаційної системи). Порушення доступності являє собою створення таких умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

- За розташуванням джерела загроз:
  - *Внутрішні* (джерела загроз розташовуються всередині системи);
  - *Зовнішні* (джерела загроз знаходяться поза системою).

- За розмірами завданого збитку:
  - *Загальні* (завдавання збитку об'єкту безпеки в цілому, заподіяння значної шкоди);

Прикладом може слугувати ситуація з вірусом «I love you», що спричинив пошкодження комп'ютерних систем у багатьох містах світу, і завдав загального збитку біля 100 мільйонів доларів США.

-
  - *Локальні* (заподіяння шкоди окремими частинами об'єкта безпеки);
  - *Приватні* (заподіяння шкоди окремим властивостям елементів об'єкта безпеки).

Яскравим прикладом є гучний «касетний скандал».

- За ступенем впливу на інформаційну систему:
  - *Пасивні* (структура і зміст системи не змінюються);
  - *Активні* (структура і зміст системи піддається змінам).

- За природою виникнення:
  - *Природні* (об'єктивні) — викликані впливом на інформаційне середовище об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини;
  - *Штучні* (суб'єктивні) — викликані впливом на інформаційну сферу людини. Серед штучних загроз у свою чергу виділяють:
    - *Ненавмисні* (випадкові) погрози, помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної та комунікаційної техніки;
    - *Навмисні* (умисні) загрози — неправомірний доступ до інформації, розробка спеціального програмного забезпечення, використовуваного для здійснення неправомірного доступу, розробка та поширення вірусних програм і т. д. Навмисні загрози зумовлені діями людей. Основні проблеми інформаційної безпеки пов'язані насамперед з умисними погрозами, оскільки вони є головною причиною злочинів і правопорушень.

За результатами, які визначили фахівці з інформаційної безпеки досліджень, понад 65 % шкоди, що наноситься інформаційним ресурсам, є наслідком ненавмисних помилок. Це є підставою для акцентування уваги на ефективнішому впровадженні комп'ютерних систем для забезпечення безпеки. Так, Національним інститутом стратегічних досліджень була запропонована програма «Електронна Україна».

У цьому плані небезпечними є співробітники спецслужб, які, маючи доступ до секретної інформації з певних причин невдоволення, роблять інформацію загальнодоступною. Одним із таких прикладів є дія колишнього генерала СБУ, одного з керівників ГУР України Валерія Кравченка, який 18 лютого 2004 року, маючи доступ до секретних матеріалів, безпідставно надав до них доступ іншим особам, зокрема журналістам «Deutsche Welle».

Класифікація джерел загроз інформаційної безпеки

Носіями загроз безпеки інформації є джерела загроз. Як джерела загроз можуть виступати як суб'єкти (особистість), так і об'єктивні прояви, наприклад, конкуренти, злочинці, корупціонери, адміністративно-управлінські органи. Джерела загроз переслідують при цьому наступні цілі: ознайомлення з охоронюваними відомостями, їх модифікація в корисливих цілях і знищення для нанесення прямого матеріального збитку.

- Всі джерела загроз інформаційної безпеки можна поділити на три основні групи:
  - *Обумовлені діями суб'єкта (антропогенні джерела)* — суб'єкти, дії яких можуть призвести до порушення безпеки інформації, дані дії можуть бути

кваліфіковані як навмисні або випадкові злочини. Джерела, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішніми, так і внутрішніми. Ці джерела можна спрогнозувати, і прийняти адекватні заходи.

- *Обумовлені технічними засобами (техногенні джерела)* — ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. Дані джерела загроз інформаційній безпеці, також можуть бути як внутрішніми, так і зовнішніми.
- *Стихійні джерела* — дана група об'єднує обставини, що становлять непереборну силу (стихійні лиха або інші обставини, які неможливо передбачити або запобігти чи можливо передбачити, але неможливо запобігти), такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз абсолютно не піддаються прогнозуванню і тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми по відношенню до захищеного об'єкта і під ними, як правило, розуміються природні катаклізми.

Порушники інформаційної безпеки

Під *порушником інформаційної безпеки* розуміється особа, яка в результаті навмисних або ненавмисних дій може завдати шкоди інформаційних ресурсів підприємства.

Під атакою на ресурси корпоративної мережі розуміється спроба нанесення шкоди інформаційних ресурсів систем, підключених до мережі. Атака може здійснюватися як безпосередньо порушником, так і опосередковано, за допомогою процесів, що виконуються від імені порушника, або шляхом впровадження в систему програмних або апаратних закладок, комп'ютерних вірусів, троянських програм і т. т. Всі порушники за ознакою приналежності до підрозділів, що забезпечують функціонування інформаційної системи (ІС), діляться на *зовнішніх і внутрішніх.*

Внутрішні порушники. Внутрішнім порушником може бути особа з наступних категорій співробітників обслуговуючих підрозділів: – обслуговуючий персонал (системні адміністратори, адміністратори БД, адміністратори додатків і т.п., що відповідають за експлуатацію і супровід технічних і програмних засобів); – програмісти, відповідальні за розробку та супровід системного і прикладного ПЗ; – технічний персонал (робітники підсобних приміщень, прибиральниці і т. п.); – співробітники бізнес підрозділів підприємства, яким надано доступ в приміщення, де розташовано комп'ютерне або телекомунікаційне обладнання. Передбачається, що несанкціонований доступ на об'єкти системи сторонніх осіб виключається заходами фізичного захисту (охорона території, організація пропускного режиму і т. П.).

Припущення про кваліфікацію внутрішнього порушника формулюються таким чином: – внутрішній порушник є висококваліфікованим фахівцем у галузі розробки та експлуатації ПЗ і технічних засобів;

– знає специфіку завдань, що вирішуються обслуговуючими підрозділами ІС підприємства;

– є системним програмістом, здатним модифікувати роботу операційних систем;

– правильно представляє функціональні особливості роботи системи і процеси, пов'язані зі зберіганням, обробкою і передачею критичної інформації;

– може використовувати як штатне обладнання і ПЗ, наявні в складі системи, так і спеціалізовані засоби, призначені для аналізу і злому комп'ютерних систем. Залежно від способу здійснення доступу до ресурсів системи та надаються їм повноважень внутрішні порушники поділяються на п'ять категорій.

Категорія А: не зареєстровані в системі особи, які мають санкціонований доступ в приміщення з обладнанням. Особи, що відносяться до категорії А можуть: мати доступ до будь фрагментам інформації, що розповсюджується по внутрішніх каналах зв'язку корпоративної мережі; розташовувати будь-якими фрагментами інформації про топологію мережі, про використовувані комунікаційних протоколах і мережевих сервісах; розташовувати іменами зареєстрованих користувачів системи і вести розвідку паролів зареєстрованих користувачів.

Категорія В: зареєстрований користувач системи, що здійснює доступ до системи з віддаленого робочого місця. Особи, що відносяться до категорії В: своєму розпорядженні всі можливості осіб, які належать до категорії А; знають, принаймні, одне легальне ім'я доступу; володіють усіма необхідними атрибутами, що забезпечують доступ до системи (наприклад, паролем); мають санкціонований доступ до інформації, що зберігається в БД і на файлових серверах корпоративної мережі, а також на робочих місцях користувачів. Повноваження користувачів категорії В з доступу до інформаційних ресурсів корпоративної мережі підприємства повинні регламентуватися політикою безпеки, прийнятої на підприємстві.

Категорія С: зареєстрований користувач, який здійснює локальний або віддалений доступ до систем входять до складу корпоративної мережі. Особи, що відносяться до категорії С: володіють всіма можливостями осіб категорії В; мають інформацію про топології мережі, структурі БД і файлових систем серверів; мають можливість здійснення прямого фізичного доступу до технічних засобів ІС.

Категорія D: зареєстрований користувач системи з повноваженнями системного (мережевого) адміністратора. Особи, що відносяться до категорії D: володіють всіма можливостями осіб категорії С; володіють повною інформацією про системний і прикладному програмному забезпеченні ІВ; володіють повною інформацією про технічні засоби та конфігурації мережі; мають доступ до всіх технічних і програмних засобів ІС і володіють правами налаштування технічних засобів і ПЗ. Концепція безпеки вимагає підзвітності осіб, які належать до категорії D та здійснення незалежного контролю над їх діяльністю.

Категорія Е: програмісти, відповідальні за розробку та супровід загальносистемного і прикладного ПЗ, використовуваного в ІС. Особи, що відносяться до категорії Е: володіють можливостями внесення помилок, програмних закладок, установки троянських програм і

вірусів на серверах корпоративної мережі; можуть розташовувати будь-якими фрагментами інформації про топологію мережі і технічних засобах ІС. Зовнішні порушники. До зовнішніх порушників належать особи, перебування яких в приміщеннях з обладнанням без контролю з боку співробітників підприємства неможливо. Зовнішній порушник: здійснює перехоплення, аналіз і модифікацію інформації, переданої по лініях зв'язку, які проходять поза контрольованої території; здійснює перехоплення і аналіз електромагнітних випромінювань від устаткування ІС. Припущення про кваліфікацію зовнішнього порушника формулюються таким чином:

– є висококваліфікованим фахівцем у галузі використання технічних засобів перехоплення інформації;

– знає особливості системного і прикладного ПЗ, а також технічних засобів ІС;

– знає специфіку завдань, що вирішуються ІС;

– знає функціональні особливості роботи системи та закономірності зберігання, обробки і передачі в ній інформації;

– знає мережеве та канальне обладнання, а також протоколи передачі даних, що використовуються в системі;

– може використовувати тільки серійно виготовляється спеціальне обладнання, призначене для знімання інформації з кабельних ліній зв'язку та з радіоканалів.

При використанні моделі порушника для аналізу можливих загроз ІБ необхідно враховувати можливість змови між внутрішніми і зовнішніми порушниками. Захист інформаційних компонентів і групи загроз. В якості об'єктів захисту виступають *наступні види* інформаційних ресурсів підприємства:

– інформація (дані, телефонні переговори і факси) передана каналами зв'язку.

– інформація, збережена в базах даних, на файлових серверах і робочих станціях, на серверах каталогів, у поштових скриньках користувачів корпоративної мережі і т.п.

– конфігураційна інформація та протоколи роботи мережевих пристроїв, програмних систем і комплексів.

Виходячи з перерахованих властивостей, всі загрози інформаційних ресурсів системи можна віднести до однієї з наступних категорій:

– загрози доступності інформації, що зберігається і оброблюваної в ІС та інформації, що передається каналами зв'язку;

– загрози цілісності інформації, що зберігається і оброблюваної в ІС та інформації, що передається каналами зв'язку;

– загрози конфіденційності інформації зберігається і оброблюваної в ІС та інформації, переданої по каналах зв'язку.

Загрози безпеці інформаційних ресурсів, з точки зору реалізації, можна розділити на наступні групи:

1. Загрози, що реалізуються з використанням технічних засобів;

2. Загрози, що реалізуються з використанням програмних засобів;

3. Загрози, що реалізуються шляхом використання технічних каналів витоку інформації.

1. *Загрози, що реалізуються з використанням технічних засобів*. Технічні засоби системи включають в себе приймально-передавальний і комутуюче обладнання, обладнання серверів і робочих станцій, а також лінії зв'язку. До даного класу відносяться загрози доступності, цілісності і, в деяких випадках конфіденційності інформації, що зберігається, обробляється і передається по каналах зв'язку системи, пов'язані з ушкодженнями та відмовами технічних засобів ІС, приймально-передавального і комутуючого обладнання та пошкодженням ліній зв'язку. Для технічних засобів характерні загрози, пов'язані з їх умисним або ненавмисним пошкодженням, помилками конфігурації і виходом з ладу:

– виведення з ладу (умисний чи ненавмисний);

– несанкціоноване або помилкове зміна конфігурації активного мережного обладнання та приймально-передавального обладнання;

– фізичне пошкодження технічних засобів, ліній зв'язку, мережевого і каналоутвоюючого обладнання;

– перебої в системі електроживлення;

– відмови технічних засобів;

– установка неперевірених технічних засобів або заміна що вийшли з ладу апаратних компонент на неідентичні компоненти;

– розкрадання технічних засобів і довготривалих носіїв конфіденційної інформації внаслідок відсутності контролю над їх використанням та зберіганням.

В якості джерел загроз безпеці для технічних засобів системи виступають як зовнішні і внутрішні порушники, так і природні явища. Серед джерел загроз для технічних засобів можна відзначити:

– стихійні лиха;

– пожежа;

– крадіжка обладнання;

– саботаж;

– помилки обслуговуючого персоналу;

– тероризм і т. п.

2. *Загрози, що реалізуються з використанням програмних засобів*. Це найбільш численний клас загроз конфіденційності, цілісності та доступності інформаційних ресурсів, пов'язаний з отриманням несанкціонованого доступу до інформації, що зберігається і оброблюваної в системі, а також передається по каналах зв'язку, за допомогою використання можливостей, що надаються ПО ІВ. Більшість розглянутих в цьому класі загроз реалізується шляхом здійснення локальних або віддалених атак на інформаційні ресурси системи внутрішніми і зовнішніми зловмисниками. Результатом успішного здійснення цих загроз стає отримання несанкціонованого доступу до інформації БД і файлових систем корпоративної мережі, даних, що зберігаються на АРМ операторів, конфігурації маршрутизаторів та іншого активного мережного обладнання. У цьому класі розглядаються такі основні види загроз:

– впровадження вірусів і інших руйнуючих програмних дій;

– порушення цілісності виконуваних файлів;

– помилки коду і конфігурації ПО, активного мережевого обладнання;

– аналіз і модифікація ПЗ;

– наявність в ПО декларованих можливостей, залишених для налагодження, або зумисне впроваджених;

– спостереження за роботою системи шляхом використання програмних засобів аналізу мережевого трафіку і утиліт ОС, що дозволяють отримувати інформацію про систему і про стан мережних з'єднань;

– використання вразливостей ПЗ для злому програмного захисту з метою отримання несанкціонованого доступу до інформаційних ресурсів або порушення їх доступності;

– виконання одним користувачем несанкціонованих дій від імені іншого користувача («маскарад»);

– розкриття, перехоплення і розкрадання секретних кодів і паролів;

– читання залишкової інформації в ОП комп'ютерів і на зовнішніх носіях;

– помилки введення керуючої інформації з АРМ операторів в БД;

– завантаження та встановлення в системі не ліцензійного, неперевіреного системного і прикладного ПЗ;

– блокування роботи користувачів системи програмними засобами. Окремо слід розглянути загрози, пов'язані з використанням мереж передачі даних. Даний клас загроз характеризується отриманням внутрішнім або зовнішнім порушником мережевого доступу до серверів БД і файлових серверів, маршрутизаторів і активного мережевого обладнання. *Тут виділяються наступні види загроз,* характерні для КСПД підприємства:

– перехоплення інформації на лініях зв'язку шляхом використання різних видів аналізаторів мережевого трафіку;

– заміна, вставка, видалення або зміна даних користувачів в інформаційному потоці;

– перехоплення інформації (наприклад, користувача паролів), переданої по каналах зв'язку, з метою її подальшого використання для обходу засобів мережевої аутентифікації;

– статистичний аналіз мережевого трафіку (наприклад, наявність або відсутність певної інформації, частота передачі, напрям, типи даних і т. п.). В якості джерел загроз безпеці для технічних засобів системи виступають як зовнішні і внутрішні порушники.

3. *Загрози витоку інформації технічними каналами зв'язку*. Види технічних каналів витоку інформації. При проведенні робіт з використанням конфіденційної інформації та експлуатації технічних засобів ІС можливі наступні канали витоку або порушення цілісності інформації або працездатності технічних засобів:

– побічні електромагнітні випромінювання інформативного сигналу від технічних засобів і ліній передачі інформації;

– акустичне випромінювання інформативного мовного сигналу або сигналу, обумовленого функціонуванням технічних засобів обробки інформації;

– несанкціонований доступ до інформації, що обробляється в автоматизованих системах;

– розкрадання технічних засобів з зберігається в них інформацією або окремих носіїв інформації;

– перегляд інформації з екранів дисплеїв і інших засобів її відображення за допомогою оптичних засобів;

– вплив на технічні чи програмні засоби з метою порушення цілісності (знищення, спотворення) інформації, працездатності технічних засобів.

Найбільшу небезпеку в даний час для промислових підприємств представляють технічні засоби розвідки:

– акустична розвідка;

– розвідка побічних електромагнітних випромінювань і наведень електронних засобів обробки інформації (далі - ПЕМВН);

– в окремих ситуаціях, можуть використовуватися: телевізійна, фотографічна і візуальна оптична розвідка, що забезпечує добування інформації, що міститься в зображеннях об'єктів, одержуваних у видимому діапазоні електромагнітних хвиль з використанням телевізійної апаратури. Крім перехоплення інформації технічними засобами розвідки можливо ненавмисне влучення конфіденційної інформації до осіб, які не допущеним до неї, але знаходяться в межах контрольованої зони.

Витік інформації можлива за такими каналами: – радіоканали; – ІЧ-канал;

– ультразвуковий канал; – дротові лінії.

В якості провідних ліній при передачі інформації до зовнішніх засобам реєстрації можуть бути використані:

– мережі змінного струму; – лінії телефонного зв'язку; – радіотрансляційні й технологічні (пожежної, охоронної сигналізації, кабелі телеантен і т.п.) лінії; – спеціально прокладені провідні лінії.

При застосуванні лазерної апаратури дистанційного прослуховування, що фіксує інформативні коливання скла у вікнах приміщень, можливий з'їм акустичної інформації з виділених приміщень, в яких встановлені елементи системи. В якості джерел загроз безпеці для технічних засобів системи виступають як зовнішні і внутрішні порушники, оснащені спеціалізованими засобами технічної розвідки. Таким чином, концепція захисту інформаційної безпеки підприємства повинна бути призначена для вирішення наступних завдань: – захисту зовнішнього периметра корпоративної мережі підприємства від загроз з боку зовнішніх мереж за рахунок використання міжмережевого екранування, контролю віддаленого доступу та моніторингу інформаційних взаємодій. – захисту корпоративних серверів за рахунок використання механізмів управління доступом до серверів баз даних, файловим, інформаційним і поштових серверів, реєстрації та обліку подій, пов'язаних із здійсненням доступу до ресурсів корпоративних серверів, механізмів моніторингу та аудиту безпеки. – комплексного антивірусного захисту систем, що входять до складу корпоративної мережі за рахунок розподілу антивірусних засобів (антивірусних сканерів, резидентних антивірусних моніторів і файлових ревізорів.

Методи забезпечення інформаційної безпеки

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 НБ 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. У числі даних методів причинних зв'язків можна назвати наступні: 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. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють:

- 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.

Виділяють декілька типів методів забезпечення інформаційної безпеки:

- однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;
- 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;
- 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;
- 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. До таких стадій належать: 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.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також переслідуваних цілей. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю по забезпеченню інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів по нейтралізації інформаційних загроз. Саме суспільство почасти використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління інформаційною безпекою, не на достатньому рівні проводиться підготовка відповідних фахівців для системи управління НБ.

Вельми важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні індивіда, суспільства і організації заважає розповсюджений міф про те, що захист інформації і криптографія одне й те саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпека лише ототожнюються із захистом інформації шляхом Я шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. Отже, система має відповідно реагувати і гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що користувач буде позбавлений можливості своєчасного і швидкого доступу до цих даних та інформації. Саме тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Втім не слід плекати надію на створення абсолютної системи інформаційної безпеки, оскільки, як зазначалося нами вище, ми стоїмо на тій позиції, що загроза та небезпека є атрибутивними компонентами системи інформаційної безпеки, отже, їх існування та реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою, і водночас слугують імпульсом до вдосконалення, тобто до розвитку. Отже, важливим метод забезпечення інформаційної безпеки е метод розвитку.

Захист інформації не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна і залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторах загрози, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє достатньо точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз тощо. Мета якісної оцінки ризиків — ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує

систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів. При чому аналіз подій в світі надає усі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинених країн.

Також можна зазначити на метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно проводяться оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак в ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення відіграє метод дихотомії. Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як у напряму надання певного впливу на джерело загрози, так і в напряму укріплення об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша — сукупністю заходів по забезпеченню інформаційної безпеки об'єкта.

Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберітеються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного і програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

Методи впливу на інформаційну інфраструктуру можуть бути поділені на інформаційні та неінформаційні. Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, систем автоматизованої обробки інформації, і таким чином, на попередження нанесення шкоди предметам суспільних відносин, що захищаються.

У цілому ж слід зазначити, що вибір цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

Огляд законодавства в галузі інформаційної безпеки

Таким чином, з урахуванням викладеного вище щодо поняття системи забезпечення інформаційної безпеки, основ її формування та функціонування, змісту та призначення, мети,

завдань, функцій та методів забезпечення, а також з урахуванням напрацювань з даних та інших споріднених питань, структура даної системи має наступний вигляд:

* стратегічний рівень управління інформаційною безпекою — Рада національної безпеки і оборони України та Кабінет Міністрів України;

• тактичний рівень управління — центральні органи виконавчої влади.

Міністерства: Міністерство аграрної політики України; Міністерство внутрішніх справ України; Міністерство охорони навколишнього природного середовища України, Міністерство економіки України, Міністерство закордонних справ України, Міністерство культури і туризму України, Міністерство оборони України, Міністерство охорони здоров'я України, Міністерство освіти і науки України, Міністерство у справах молоді та спорту, Міністерство палива та енергетики України, Міністерство праці та соціальної політики України, Міністерство промислової політики України, Міністерство транспорту та зв'язку України, Міністерство України з питань надзвичайних ситуацій у справах захисту населення від наслідків Чорнобильської катастрофи, Міністерство фінансів України, Міністерство юстиції України;

Центральні органи виконавчої влади зі спеціальним статусом:Державна судова адміністрація України, Головне управління державної служби України, Пенсійний фонд України, Державний комітет статистики України, Державна комісія з цінних паперів та фондового ринку України, Державна служба охорони України, Служба безпеки України, Фонд державного майна України, Національна комісія регулювання електроенергетики України, Державний комітет ядерного регулювання України, Державний комітет України з питань регуляторної політики та підприємництва, Державна податкова адміністрація України, Державна митна служба України, Антимонопольний комітет України, Державний департамент України з питань виконання покарань, Державна прикордонна служба України, Державна комісія з регулювання ринків фінансових послуг України, Державна служба експортного контролю України.

Державні комітети та інші центральні органи виконавчої влади, статус яких прирівнюється до Державного комітету У країни: Державний комітет України з державного матеріального резерву, Державний комітет архівів України, Державний комітет України з нагляду за охороною праці, Державний комітет України з будівництва та архітектури, Державний комітет України з питань житлово-комунального господарства, Державний комітет України по водному господарству, Державний комітет України по земельних ресурсах, Державний комітет телебачення і радіомовлення України, Державний комітет лісового господарства України, Державний комітет України у справах національностей та міграції, Державний комітет статистики України, Національне космічне агентство України, Державна служба автомобільних доріг України.

Інші центральні органи та установи. Інформаційний центр Міністерства юстиції України, Головне контрольно-ревізійне управління України, Вища атестаційна комісія, Головне управління реєстрації та ліцензування, Державне казначейство України, Національний інститут стратегічних досліджень,

Департамент спеціальних телекомунікаційних систем та захисту інформації, Український державний центр радіочастот, Укравіатранс, Департамент ДАІ МВС України, Центр медичної статистики, Національний олімпійський комітет, Рахункова палата України, Державний департамент продовольства України, Національний Депозитарій України, Експоцентр України, Національний банк України, Рада підприємців України при Кабінеті Міністрів України, Державний департамент інтелектуальної власності, Вища рада юстиції, Державна служба лікарських засобів і виробів медичного призначення.

Центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через відповідних міністрів;

- через Міністра економіки України: Державний комітет України з енергозбереження;
- через Міністра праці та соціальної політики України: Державний комітет України у справах ветеранів;
- через Міністра транспорту та зв'язку України: Державна служба автомобільних доріг України;
- через Міністра фінансів України: Головне контрольно-ревізійне управління України, Державне казначейство України;
- через Міністра юстиції України: Державний комітет України у справах релігій.
- **оперативний рівень** — місцеві органи виконавчої влади. Основним змістом системи забезпечення інформаційної безпеки є реалізація сукупності науково-обґрунтованих і апробованих на практиці з урахуванням світового і вітчизняного досвіду заходів у контексті реалізації державної політики інформаційної безпеки.

Суттєвим є той факт, що забезпечення інформаційної безпеки є обов'язковим для усіх інших державних органів і організацій, яке вони здійснюють у межах своєї компетенції самостійно, а також при зверненні основних суб'єктів забезпечення національної безпеки.

Систему забезпечення інформаційної безпеки складає певне коло суб'єктів, які діють відповідно до поставлених завдань і, виконуючи конкретні функції, ґрунтуючись при їх здійсненні визначеними принципами, застосовуючи адекватні методи, утворюють один з вагомих елементів загальної системи національної безпеки.

Розглянемо компетенцію основних складових компонентів системи забезпечення інформаційної безпеки.

Кабінет Міністрів України як вищий орган у системі органів виконавчої влади, відповідальний перед Президентом України та підконтрольний і підзвітний Верховній Раді України у межах, передбачених статтями 85, 87 Конституції України, відповідно до ст. 116 Конституції України, а також ст. 9 Закону України "Про основи національної безпеки України":

- забезпечує інформаційний суверенітет України, здійснення внутрішньої і зовнішньої інформаційної політики держави, виконання Конституції і законів України, актів Президента України, що стосуються інформаційної безпеки;
- вживає заходів щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері;
- забезпечує проведення державної політики інформаційної безпеки;
- спрямовує і координує роботу усієї системи органів державного управління з питань, що стосуються інформаційної безпеки.

Окрім цього, з аналізу нормативно-правової бази, що регулює діяльність Кабінету Міністрів України, можна виокремити також і інші функції та завдання в сфері інформаційної безпеки, серед яких можна виділити наступні:

- визначає потреби в витратах на забезпечення інформаційної безпеки, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах;
- організовує розроблення і виконання державних програм з розвитку інформаційної інфраструктури органів державного управління;
- здійснює передбачені законодавством заходи щодо формування, розміщення, фінансування та виконання державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб органів, що забезпечують інформаційну безпеку;
- встановлює порядок надання суб'єктам забезпечення інформаційної безпеки у користування державного майна, засобів зв'язку і радіочастотного ресурсу, комунікацій, інших об'єктів інфраструктури держави, навігаційної, топогеодезичної, метеорологічної, гідрографічної та іншої інформації;
- здійснює загальнодержавні заходи щодо забезпечення живучості об'єктів інформаційної інфраструктури;
- забезпечує комплектування особовим складом сили забезпечення інформаційної безпеки;
- утворює, реорганізовує, ліквідовує науково-дослідні установи, навчальні заклади та окремі кафедри (відділення, факультети) суб'єктів забезпечення інформаційної безпеки;
- забезпечує реалізацію права на соціально-економічний захист відповідно до законодавства України, що регламентує діяльність окремих суб'єктів забезпечення інформаційної безпеки;
- здійснює у визначених законом випадках регулювання господарської діяльності у суб'єктах забезпечення інформаційної безпеки;
- встановлює відповідно до закону порядок реалізації та утилізації об'єктів інформаційної інфраструктури, інформаційних ресурсів;
- забезпечує здійснення, передбачених законодавством заходів, щодо цивільної оборони України, надання військової допомоги іншим державам, направлення підрозділів Збройних сил України до інших держав, допуску та умов

перебування підрозділів збройних сил інших держав на території України та участі України в міжнародних миротворчих операціях;

- контролює виконання законів у сфері оборони, здійснює відповідно до законів інші заходи щодо забезпечення обороноздатності України, координує і контролює їх виконання та несе, в межах своїх повноважень, відповідальність за забезпечення оборони України.

Міністерства та інші центральні органи виконавчої влади в межах своїх повноважень, наявних засобів бюджетного і позабюджетного фінансування:

- забезпечують реалізацію законів України, указів та розпоряджень Президента України, концепцій, доктрин, програм, постанов органів державного управління у сфері інформаційної безпеки;
- забезпечують створення, підтримку в готовності і застосування сил та засобів забезпечення інформаційної безпеки, а також управління їх діяльністю;
- у межах своєї компетенції розробляють нормативні правові акти в інформаційній сфері і представляють їх Президентові України та Кабінету Міністрів України;
- вносять в органи виконавчої влади пропозиції по удосконалення функціонування системи забезпечення інформаційної безпеки України;
- керують діяльністю підвідомчих організацій з планування і проведення заходів по забезпеченню інформаційної безпеки;
- забезпечують дотримання прав і законних інтересів громадян, організацій і держави, законів та інших нормативно-правових актів в інформаційній сфері;
- притягують до відповідальності посадових осіб, дії яких призводять до порушення національних інтересів в інформаційній сфері, створюють умови або безпосередню загрозу інформаційній безпеці України.

Відповідно до ст. 13 Закону України "Про місцеві державні адміністрації" до відання місцевих державних адміністрацій у межах і формах, визначених Конституцією і законами України, належить вирішення питань:

1) забезпечення законності, охорони прав, свобод і законних інтересів громадян;

2) соціально-економічного розвитку відповідних територій;

3) бюджету, фінансів та обліку;

4) управління майном, приватизації та підприємництва;

5) промисловості, сільського господарства, будівництва, транспорту і зв'язку;

6) науки, освіти, культури, охорони здоров'я, фізкультури і спорту, сім'ї, жінок, молоді та неповнолітніх;

8) зовнішньоекономічної діяльності;

9) оборонної роботи та мобілізаційної підготовки;

10) соціального захисту, зайнятості населення, праці та заробітної плати.

При чому місцеві державні адміністрації вирішують й інші питання, віднесеш законами до їх повноважень.

Цікавим є і той факт, що Кабінет Міністрів України в межах, визначених законами України, може передавати місцевим державним адміністраціям окремі повноваження органів виконавчої влади вищого рівня.

Передача місцевим державним адміністраціям повноважень інших органів супроводжується передачею їм відповідних фінансових, матеріально-технічних та інших ресурсів, необхідних для здійснення цих повноважень.

До безпосередньої компетенції місцевих державних адміністрацій в сфері забезпечення інформаційної безпеки можна віднести:

1) забезпечує виконання Конституції та законів України, рішень Конституційного Суду України, актів Президента України, Кабінету Міністрів України, інших органів державної влади в сфері забезпечення інформаційної безпеки;

2) забезпечує здійснення заходів щодо охорони громадської безпеки, громадського порядку, боротьби зі злочинністю в інформаційній сфері;

3) забезпечує розгляд звернень громадян та їх об'єднань, контролює стан цієї роботи в органах місцевого самоврядування, на підприємствах, в організаціях і установах, розташованих на відповідній території;

4) здійснює заходи щодо організації правового інформування та інформаційного виховання населення;

5) проводить роботу, пов'язану з розробленням та здійсненням заходів щодо інформаційного забезпечення біженців, а також депортованих осіб, які добровільно повертаються в регіони їх колишнього проживання;

6) забезпечує виконання законодавства щодо національних меншин і міграції, про свободу думки і слона, свободу світогляду і віросповідання;

7) оголошує у разі стихійного лиха, аварій, катастроф, епідемій, енізоотій, пожеж, інших надзвичайних подій зони надзвичайної ситуації; здійснює передбачені законодавством заходи, пов'язані із забезпеченням інформаційної безпеки, захистом інформаційних прав особи;

8) здійснюють інформаційне супроводження діяльності аварійно-рятувальних служб за місцем їх дислокації, під час прямування до зон надзвичайних ситуацій та під час ліквідації надзвичайних ситуацій, зокрема у поданні їм необхідної інформації, засобів зв'язку та інших матеріальних засобів і послуг;

9) погоджує проект плану проведення потенційно небезпечних заходів в умовах присутності цивільного населення за участю особового складу Збройних сил України, інших військових формувань та правоохоронних органів з використанням озброєння і військової техніки; взаємодіє з органами військового управління під час планування та проведення таких заходів з метою запобігання і недопущення надзвичайних ситуацій та ліквідації їх наслідків;

10) забезпечує своєчасне інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій під час проведення потенційно небезпечних заходів в умовах присутності цивільного населення за участю особового складу Збройних сил України, інших військових формувань та правоохоронних органів з використанням озброєння і військової техніки;

11) розглядає справи про адміністративні правопорушення, віднесені до її відання, утворює адміністративні та спостережні комісії, координує їх діяльність;

12) здійснює разом з відповідними виконавчими органами рад підготовку і внесення в установленому порядку на розгляд ради пропозицій, погоджених з відповідними головними управліннями, управліннями Міністерства внутрішніх справ України в Автономній Республіці Крим, областях, містах Києві та Севастополі, щодо утворення, реорганізації або ліквідації місцевої міліції, чисельності її працівників згідно з нормативами, затвердженими Міністерством внутрішніх справ України, витрат на утримання та матеріально-технічне забезпечення діяльності місцевої міліції, навчання її працівників, створення ДЛЯ них необхідних житлово-побутових умов.

Основне завдання по реалізації державної політики у сфері інформаційної безпеки покладено на органи виконавчої влади, які здійснюють на основі законодавства державне управлівня.

Компетенція органів виконавчої влади у сфері забезпечення інформаційної безпеки полягає у виконанні законодавства У краї ни, рішень Президента України і Кабінету Міністрів України у зазначеній сфері. Предмети ведення органів виконавчої влади в області забезпечення інформаційної безпеки визначаються Президентом України і Кабінетом Міністрів Україна. Зміст владних повноважень органів виконавчої влади полягає у тому, щоб приймати в рамках предметів власного ведення відповідні нормативні правові акти, здійснювати правозастосовчу практику, готувати пропозиції по реалізації спільно з іншими органами виконавчої влади основних напрямів політики національної безпеко в інформаційній сфері.

Компетенція міжвідомчих і державних комісій з різних аспектів забезпечення інформаційної безпеки, які створюються Президентом і Кабінетом Міністрів, полягає передусім у забезпеченні узгодженості діяльності усієї системи органів державного управління. Предмети їх ведення визначаються положеннями про них, а владні повноваження, як правило, обмежуються прийняттям рішень, що носять рекомендаційний характер.

Особливість реалізації функцій забезпечення інформаційної безпеки полягає у тому, що кожний орган держави здійснює власну діяльність на базі використання інформаційної інфраструктури суспільства, виробляє і споживає інформаційні ресурси, має певні відносини із громадянами і як власник інформаційних ресурсів і тих, що складають інформаційну інфраструктуру, мас вживати певні дії по забезпеченню збереження ресурсів і безпеки функціонування інформаційних і телекомунікаційних систем, мереж зв'язку, систем управління.

Відповідно до Закону України "Про основи національної безпеки України" до основних напрямів політики національної безпеки в інформаційній сфері належать:

• забезпечення інформаційного суверенітету України;

* вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

* активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;

- абезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Державна політика національної безпеки в інформаційній сфері має створювати умови для реалізації конституційного права громадян своєї держави вільно отримувати і використовувати інформацію для вирішення таких важливих завдань, як формування національного інформаційного простору, включення його до світового інформаційного простору на засадах забезпечення інформаційного суверенітету та інформаційної безпеки і формування демократично орієнтованої свідомості.

Головною метою державної політики національної безпеки в інформаційній сфері є створення необхідних економічних і соціокультурних умов, правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних

інформаційних ресурсів у всіх сферах життєдіяльності особи, суспільства і держави як органічного організму.

У цілому ж напрями державної політики мають відповідати загрозам НБ в інформаційній сфері, а також враховувати потенціал системи забезпечення, тобто основні завдання, які вона не тільки зобов'язана, а й може виконувати. Відтак, напрями даної політики можуть також розглядатися крізь призму завдань системи забезпечення інформаційної безпеки, які ми розглядали вище.

На мій погляд, також доцільно прискорити розроблення і прийняття Доктрини інформаційної безпеки України, яка має розвивати положення Концепції національної безпеки України відповідно до інформаційної сфери. Теоретичні питання щодо формування доктрин викладені нами у 3 розділі.

Основним призначенням доктрини інформаційної безпеки є закріплення методології і формування єдиної системної мети прийняття усього циклу законодавчих актів у сфері забезпечення інформаційної безпеки. Дані акти мають бути спрямовані на врегулювання суспільних відносин з наступного кола ключових питань:

- • використання інформаційної структури і телекомунікацій;
- • доступу до інформації;
- • захисту інформації від несанкціонованого доступу і від її витоку по технічних каналах;
- • захисту громадян, суспільства і держави від хибної недобросовісної інформації;
- • захисту інформації телекомунікаційних мереж від неправомірних дій;
- • забезпечення техногенної безпеки, у тому числі в області її інформаційних аспектів і боротьби з технологічним тероризмом.

До основних напрямів дій Кабінету Міністрів України можна віднести наступні:

- • розроблення та підписання двосторонніх і багатосторонніх угод у сфері інформаційної безпеки;
- • розроблення та організація прийняття Доктрини інформаційної безпеки;
- • здійснювати заходи щодо підготовки нормативно-правових актів і удосконалення вже існуючих, що забезпечують реалізацію законодавства в сфері інформаційної безпеки;
- • з метою розвитку і удосконалення системи підготовки кадрів з інформаційної безпеки з України звернутися до Європейської комісії з питань включення даної системи до числа пріоритетних напрямів програми технічної допомоги ТАСК5.

До основних напрямів дій керівників органів виконавчої влади можна віднести наступні:

- • всіляко сприяти проведенню наукових досліджень з проблем забезпечення інформаційної безпеки;
- • зосередити увагу на захисті матеріально-технічних об'єктів, які складають фізичну основу інформаційних ресурсів, а також інформаційних технологій;
- • забезпечувати нормальне і безперебійне функціонування баз даних і телекомунікаційних систем;
- • вживати заходів по захисту інформації від її витоку по технічних каналах, від несанкціонованого доступу, викривлення або знищення;
- • виявлення технічних пристроїв і програм, які становлять небезпеку для нормального функціонування інформаційно-телекомунікаційних систем, попередження перехоплення інформації по технічних каналах зв'язку, застосування криптографічних засобів захисту інформації при її зберіганні, обробленні та передачі по каналах зв'язку, контроль за виконанням спеціальних вимог із захисту Інформації;

■ здійснювати розвиток систем сертифікації засобів інформатизації, програмних продуктів, засобів захисті інформації;

■ розвивати та вдосконалювати систему ліцензування діяльності і забезпечення інформаційної безпеки і міжнародного інформаційного обміну;

- • здійснювати контроль за діями персоналу в захищених інформаційних системах;
- • удосконалювати і розвивати систему підготовки і перепідготовки кадрів у сфері інформаційної безпеки з урахуванням передового Міжнародного досвіду;
- • завершити формування і удосконалення системи забезпечення інформаційної безпеки, підвищення її дієздатності;
- • посилити правозастосовчу діяльність органів державної влади, включаючи попередження і припинення правопорушень в інформаційній сфері, а також виявлення, викриття і притягнення до відповідальності осіб, що вчинили злочини або інші правопорушення у цій сфері;
- • розробляти, розповсюджувати, використовувати і удосконалювати засоби захисту інформації і методи контролю ефективності цих засобів, розвивати захищені телекомунікаційні системи, підвищувати надійність спеціального програмного забезпечення;
- • розробляти та реалізовувати комплексні цільових програми забезпечення інформаційної безпеки, що стимулюють діяльність у сфері захисту інформації і визначення порядку фінансування;
- • удосконалювати системи фінансування робіт, пов'язаних із реалізацією правових і організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних та юридичних осіб;
- • забезпечувати технологічну незалежність від зарубіжних виробників у найважливіших сферах інформатизації, телекомунікації та зв'язку.

Перелік напрямів державної політики не є вичерпним, водночас він має відображати реальний рівень інформаційної безпеки, котрий грунтується на виявлених і прогнозованих загрозах, а також відповідних заходах по управлінню ними.

Тематика практичних робіт та самостійної роботи

1. Практична робота № 1. Інформаційні ресурси з проблематики захисту інформації у мережі Інтернет

2. Практична робота № 2. Процес управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем

3. Практична робота № 3. Моніторинг згадувань об'єктів (інцидентів з інформаційною безпекою) у мережі Інтернет

4. Практична робота № 4. Інформаційне забезпечення кадрового менеджменту служб інформаційної безпеки на підприємстві

5. Практична робота № 5. Організація діяльності відділу управління інформаційними ресурсами та захисту інформації

6. Практична робота № 6. Планування заходів аудиту інформаційної безпеки

Лабораторна робота № 1. Тема: Інформаційні ресурси з проблематики захисту інформації у мережі Інтернет

Загальні відомості. Подання органами державної влади інформації у мережі Інтернет є одним найбільш дієвих способів взаємодії влади і суспільства.

Сайт органу державної влади є відкритим і загальнодоступним інформаційним ресурсом, використання якого здійснюється безоплатно, однак, сайт може містити також інформацію обмеженого доступу.

До сайта органу державної влади висуваються певні вимоги:
— представлення інформації про орган влади, його місцезнаходження, наявність контактної інформації, визначення умов і форм використання матеріалів сайта;
— забезпечення цілодобового контролю за працездатністю сайта;
— з метою запобігання створенню нерівних умов для різних користувачів для доступу до сайту не повинні пред'являтись завищені вимоги до апаратного і програмного забезпечення;
— дотримання принципу поваги до практики інформаційного обміну у мережі Інтернет (відсутність відповідей на звертання громадян і організацій є неприйнятною практикою); — обмеження на сайті органу державної влади інформації, джерелом якої виступають треті особи (у випадку, якщо така інформація наявна, орган влади повинен визначити межі своєї відповідальності за її повноту і достовірність);
— кожен електронний документ повинен мати власну унікальну адресу, має публікуватись інформація про дату його розміщення, а також забезпечуватись довготривале зберігання оновлюваної інформації;
— розміщення інформації про умови використання сайта.
Пошук урядових ресурсів України доцільно починати з урядового порталу України (http://www.kmu.gov.ua). Повний список адрес серверів парламентів світу представлений на сайті Міжпарламентського союзу (www.ipu.org/english/parlweb.htm). Пошук парламентської інформації України - з сайту Верховної Ради України (www.rada.kiev.ua).

Інформаційні ресурси архівів у мережі Інтернет .

Архіви зберігають найрізноманітніші види документів з усіх сфер суспільної і особистої діяльності: управлінську документацію, документи особового походження, картографічні документи, науково-технічну документацію, кіно-, фото-, фоно-, відедокументи, документи церковних конфесій тощо.

Метою функціонування сайтів архівних установ є популяризація архівної справи, розширення доступу громадян і організацій до архівних матеріалів, надання інтерактивних послуг, висвітлення діяльності архівних установ, висвітлення змісту періодичних видань з архівної справи.

Сайти архівів виконують такі функції: надання для широкого кола користувачів науково-довідкового апарату архівів, інформування про діяльність архівних закладів, надання інформації про склад і зміст архівних документів, подання законодавчої, нормативної та методичної бази функціонування архівних установ, висвітлення змісту публікацій (з повними текстами) з архівної справи.

Пошук інформації, яка надається архівами України, можна починати з порталу "Архіви України" (http://www.archives.gov.ua/). Бібліотечно-бібліографічні ресурси мережі Інтернет У мережі Інтернет представлено значну кількість бібліотечнобібліографічних інформаційних ресурсів як у вигляді бібліотечної реклами, так і з власне бібліографічною інформацією, яка міститься у електронних каталогах. Крім цього, бібліографічна інформація розташовується на серверах наукових і освітніх закладів, які представляють доступ до своєї наукової продукції – періодичним виданням у електронній формі, при чому як на бібліографічному рівні, так і на повнотекстовому. Бібліографічна інформація може надаватись також серверами видавництв та книготорговельних організацій, спеціальними службами, які забезпечують рефератами або анотаціями журнальних статей та інших друкованих матеріалів та ін. Сайт найбільшої бібліотеки України – Національної бібліотеки України ім. В.В. Вернадського (www.nbuv.gov.ua), який містить гіперпосилання на провідні бібліотеки світу і України.

Хід роботи: 1. Ознайомитись з урядовими, парламентськими, архівними та бібліотечними ресурсами мережі Інтернет за наведеними адресами порталів.

2. Проаналізувати представлені ресурси. Порівняти склад і структуру інформаційних ресурсів, до яких надається доступ. Скласти порівняльну таблицю (поставити знаки + та -).

Таблиця 1.1

Тип (назва) ресурсу web-адреса	Доступ до електронного каталогу або пошук по сайту	Доступ до повних текстів електронних документів	Посилання на інші інформаційні ресурси мережі Інтернет

3. Оформити звіт.

Лабораторна робота № 2. Тема: Процес управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем

Загальні відомості. У світі інформаційних технологій та наукових досліджень поняття живучості відоме як властивість, яка характеризує здатність системи (надалі розглядатимемо бізнес-процес компанії) ефективно функціонувати за умови впливу чинників дестабілізації (ЧД): збої в роботі, руйнування, компрометація тощо та відновлювати таку здатність протягом заданого проміжку часу. Згідно з цим визначенням невід'ємною складовою властивості живучості бізнес-процесу компанії є неперервність його виконання. Міжнародний стандарт ISO 27001, який визначає вимоги до систем менеджменту інформаційної безпеки (СМІБ), тлумачить неперервність функціонування як один із рекомендованих контролів у життєвому циклі СМІБ.

Отже, неперервність функціонування є не лише запорукою ефективного розроблення та впровадження СМІБ, але й дієвим способом та невід'ємною складовою процесу забезпечення властивості живучості.

За умов швидкого прогресу сучасного суспільства та високого ступеня інформатизації корпоративні мережі зв'язку (КМЗ) є основним методом збору, оброблення, зберігання та передавання інформації. Водночас, відмітимо важливість такого складового компонента КМЗ, як система захисту інформації (СЗІ), від коректності функціонування якої залежить захищеність інформаційних активів компанії. Тому наголошуємо не просто на властивості живучості організації загалом, а на забезпеченні неперервності функціонування СЗІ в КМЗ як невід'ємній та критично важливій частині ефективного та безпечного функціонування компанії, виконання її основних бізнес-процесів.

Розрізнятимемо такі основні категорії чинників дестабілізації нормальної роботи СЗІ як складової КМЗ в контексті забезпечення їхнього неперервного функціонування

− Стихійні лиха. Порушення ІБ відбувається внаслідок впливу стихійних лих (наприклад потоп, сильний вітер, блискавка, обвал тощо), що непідконтрольні людині.

− Соціальні заворушення. Порушення ІБ, яке зумовлене нестабільністю суспільства (наприклад, акти вандалізму, терористичні акти, війни тощо).

− Фізичні пошкодження. Порушення ІБ, яке зумовлене навмисним або випадковим фізичним впливом на СЗІ або її компоненти (наприклад, вогонь, вода, електростатика, вплив навколишнього середовища (забруднення, пил, корозія, замерзання), руйнування, крадіжка, втрата, невміле поводження з обладнанням / носієм інформації).

− Порушення ІБ через відмову базових компонентів СЗІ і послуг, що підтримують функціонування КМЗ (наприклад, відмова мережі електроживлення, системи кондиціонування повітря, системи водопостачання).

− Порушення ІБ внаслідок порушень, які зумовлені, наприклад, електромагнітним випромінюванням, коливаннями напруги, електронними завадами.

− Технічний збій. Порушення ІБ, спричинене відмовами СЗІ або пов’язаними з нею нетехнічними можливостями. До такого типу ризиків зараховуємо апаратний, програмний збій, перевантаження, порушення ремонтоздатності.

− Технічні атаки. Порушення ІБ, що зумовлене атакуванням КМЗ та використанням її уразливостей в конфігуруванні, протоколах, програмах тощо. Наприклад, мережеве сканування, експлуатація вразливості / бекдору, спроба входу, втручання, відмова в обслуговуванні (DOS / DDoS).

У роботі розглянуто процес управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в КМЗ як невід’ємної складової ефективної та безпечної роботи компанії.

Метою процесу управління ризиками ІБ є виявлення, контроль та мінімізація невизначеності впливу ЧД. Виділимо чотири основні етапи управління ризиками ІБ, яке здійснюється з метою забезпечення неперервності функціонування КМЗ, зокрема підсистеми СЗІ:

1. Аналіз ризику. Виявлення та оцінка ЧД, які можуть скомпрометувати ІБ важливих інформаційних активів. Дає змогу визначити профілактичні заходи щодо зниження ймовірності виникнення ЧД і визначити контрзаходи з метою успішної нейтралізації цих обмежень ще на етапі проектування.

2. Оцінка ризику. Є процесом визначення рівня ризику. Ризик традиційно обчислюватимемо як функцію важливості активів, ймовірності виникнення загрози і наявності уразливостей, величини завданого збитку.

3. Зниження ризику. Це етап, на якому реалізовуються контролі та заходи щодо запобігання визначеним ризикам, а також впроваджуються засоби відновлення у разі реалізації ризиків, що можуть порушити неперервне функціонування СЗІ.

4. Оцінка уразливостей та контролів. Аналіз основних властивостей КМЗ та виявлення тих, які можна використати з метою реалізації загрози порушення властивості живучості, а також визначення ефективності та адекватності заходів ІБ та виявлення недоліків в її реалізації.

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST 800-30, методика CRAMM та методика OCTAVE.

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, 18 зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management

Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози.

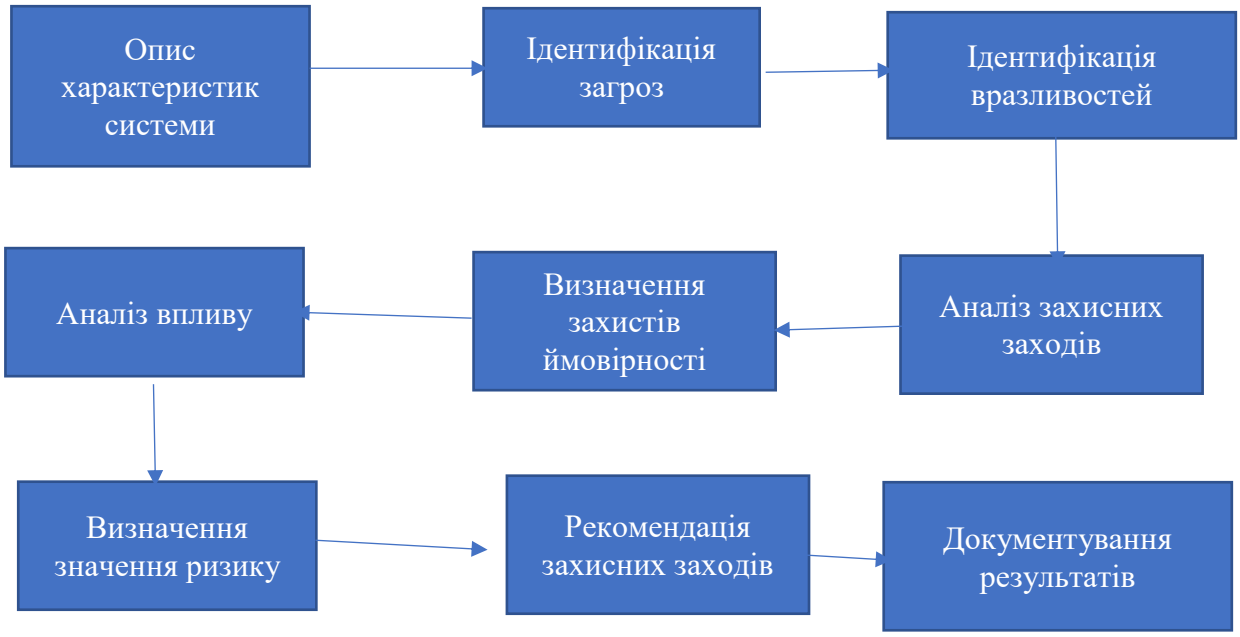
Призначення системи управління ризиками безпосередньо пов'язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800- 30, охоплює широке коло завдань, що пов'язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий "жорсткий" механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність.

Використання такої методики передбачає такі етапи: − опис характеристик системи;

− ідентифікація загроз; − ідентифікація уразливостей; аналіз наявних засобів/заходів захисту; − визначення значення ймовірності; − аналіз впливу; − визначення значення ризику; − вибір засобів/заходів захисту; − документування отриманих результатів.

Алгоритм цієї методики зображено на рис. 2.1.



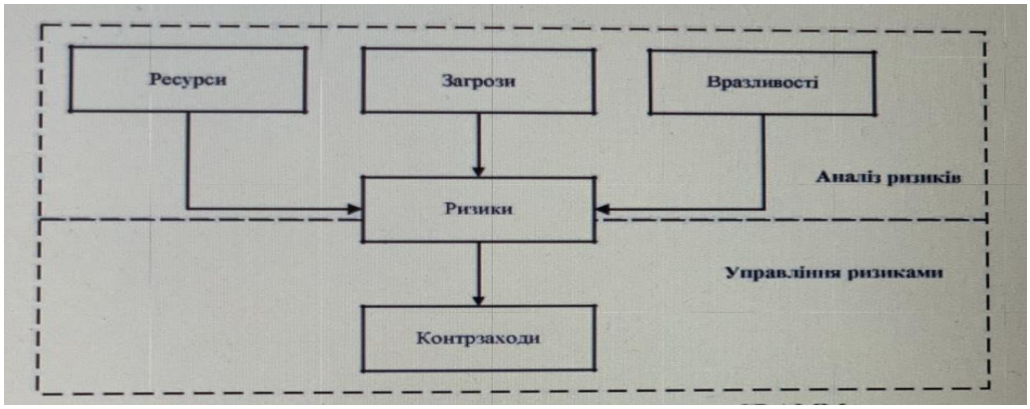
Наступною методикою, яку потрібно проаналізувати, є методика CRAMM (CCTA Risk Analysis and Managment Method), яку розробило Агентство з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за поданням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації Великобританії. За цей час CRAMM набула

популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM.

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC ("Помаранчева книга").

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: "Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?" На 20 другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки і набір звітних документів



Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей. Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності.

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи.

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних

вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз уразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних уразливостей компанії та оцінювання їх величини. На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням уразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ. Алгоритм цієї методики: Встановити критерії для оцінки ризиків - Створити перелік інформаційних активів - Ідентифікувати зміст інформаційних активів - Визначити область застосування – Визначити сценарій загроз – Визначити ризики – Проаналізувати ризики - Вибрати підходи для зниження ризиків.

Охарактеризувавши три найпоширеніші методики з управління ризиками в сфері інформаційної безпеки та здійснивши аналіз основних властивостей цих методик, визначимо основні їх переваги та недоліки, див. табл. 2.2.

Таблиця 2.2. Переваги та недоліки методик з управління ризиками ІБ

Методика	Переваги	Недоліки
NIST		
CRAMM		
OCTAVE		

Завдання: Заповнити таблицю 2.2, на основі даних аналізу переваг та недоліків NIST, CRAMM та OCTAVE

Практична робота № 3
Тема: Моніторинг згадувань об’єктів (інцидентів з інформаційною безпекою) у мережі Інтерне.

Загальні відомості. Подієвий аналіз є одним із найбільш розповсюджених методологічних засобів вивчення динаміки ситуацій з інформаційною безпекою. Методика аналізу ґрунтується на спостереженні за розвитком та інтенсивністю подій (інцидентів з інформаційною безпекою) з метою визначення тенденцій.

Моніторинг - безперервне спостерігання за станом оточуючого середовища з метою управління ним шляхом своєчасного інформування про можливості настання несприятливих, критичних або неприпустимих ситуацій у галузі ІБ.

Моніторингові дослідження широко застосовуються для вивчення різноманітних об’єктів з метою прогнозу їх розвитку. Моніторингові дослідження передбачають одержання статистичних або змістових показників, які характеризують об’єкт спостереження і які можна виміряти. Система спостережень будується на фіксації дискретних кількісних характеристик об’єкта спостереження, накопичуванні цих відомостей і на можливості шляхом інтелектуальної інтерпретації одержаних відомостей зробити висновки про якісний стан об’єкта. Моніторинг ґрунтується на спостереженні типових рис у поведінці об’єктів спостереження і на своєчасній фіксації на їх фоні різних відхилень від норми.

Хід роботи

1.Визначити об’єкт (особу або подію), відносно якого буде здійснюватися моніторинг.

2.Визначити джерела інформації (наприклад, журнали або ін.), які будуть використані як інструмент дослідження.

3.Визначити період (напр. 07.12.20..-22.02.20.. щотижня), протягом якого буде здійснюватися дослідження.

4.Протягом визначеного періоду здійснювати моніторинг згадувань об'єкта (події), кількісні показники

5. Побудувати графік. Зробити висновки щодо причин і тенденцій динаміки зафіксованих характеристик об'єкта спостереження

Практичнаробота № 4 .Тема: Інформаційне забезпечення кадрового менеджменту служб інформаційної безпеки на підприємстві.

Загальні відомості. З метою атестації, адаптації персоналу і моніторингу ефективності кадрового менеджменту служби ІБ доцільно застосовувати експертні опитування. Основним інтегральним чинником, який позитивно впливає на професійну діяльність особистості, є привабливість для неї самої виконуваної роботи. Компонентами цього чинника є:

1. Чинники прийнятності (необхідні, але не достатні): − політика фірми і адміністрації; − умови робочого оточення; − заробітна платня; − міжособистісні відносини (в т. ч. з керівництвом); − ступінь безпосереднього контролю за роботою (рівень регламентації, концепція роботи за принципами досягнення заданих цілей, за принципом виконаних завдань тощо);

2. Мотиваційні чинники (достатні для підвищення продуктивності праці): − досягнення визнаного особистого успіху; − просування по службі; − визнання результатів роботи; − високий ступінь відповідальності; − можливість творчого зростання.

Мета роботи: виконати дослідження соціально-професійних уподобань членів колективу відділу захисту інформації (служби інформаційної безпеки) і порівняти їх з результатами таких самих досліджень у США і ЕС.

Хід роботи: 1. Для оцінки відносної значущості чинників привабливості роботи необхідно виконати ранжування чинників (за 10-бальною шкалою: 1 – мінімальна значущість, 10-максимальна) і порівняти з результатами опитування працівників у США і ЕС.

2. Оцінити і порівняти ранги чинників

№ з/п	Чинники, які роблять роботу більш привабливою	Робить роботу більш привабливою					Стимулює працювати більш інтенсивно				
1	Робота без значних напружень і стресів	Працівник 1	Працівник 2	……	Працівник N	Середнє	Працівник 1	Працівник 2	……	Працівник N	Середнє
2	Зручне розташування										
3	На робочому місці немає шуму і будь-яких забруднень оточуючого середовища										
4	Робота з людьми, які викликають симпатію										
5	Хороші відносини з безпосереднім керівництвом										

6	Достатня інформація про те, що взагалі відбувається у фірмі										
7	Гнучкий темп роботи										
8	Гнучкий робочий час										
9	Значні додаткові пільги										
10	Справедливий розподіл обсягів робіт										

3.1.Виконати аналіз одержаних даних, пояснити результати. Оформити звіт.

Практична робота № 5 Тема: Організація діяльності відділу управління інформаційними ресурсами та захисту інформації

Загальні відомості. Інформаційний менеджмент представляє персонал інформаційних підрозділів як один з пріоритетних ресурсів, який реалізує інформаційну стратегію організації.

Управління інформаційним персоналом організації – комплекс управлінських заходів, які забезпечують відповідність кількісних і якісних характеристик персоналу та спрямованості і мотивації його професійної діяльності цілям і завданням організації. Система управління інформаційними ресурсами організаційно базується на розробці положення про відділ управління інформаційними ресурсами та захисту інформації.

Зміст діяльності і призначення відділу визначається, виходячи з таких підсистем загальної системи діяльностей: документно-інформаційні ресурси – управління інформаційною діяльністю – комунікації. З метою підвищення ефективності діяльності організацій пропонується введення посади CIO (Chief Information Officer) – професійного менеджера, який має системний стратегічний погляд на бізнес, поєднує компетенції менеджера і фахівця з захисту інформації, інформаційних потоків і структур, бере на себе відповідальність за формування інфраструктури для створення єдиної захищеної інформаційної системи підприємства, відповідає за організацію всіх інформаційних потоків всередині організації, за її представлення у зовнішньому середовищі, відповідає за забезпечення інформацією всіх функціональних спеціалістів компанії і керівників; має знання і навички формування і використання інформаційних ресурсів в управлінні підприємствами і бізнес-процесами. Відповідно до загальної структури організації та завдань, що перед нею постають, спрямованість діяльності відділу управління інформаційними ресурсами може визначатись у таких напрямах: відділ зв'язків з громадськістю, інформаційно-аналітичний відділ, інформаційна служба, яка працює за принципом інформаційно-технологічного підрозділу, що спеціалізується на збиранні, обробці, зберіганні та розповсюдженні документальної, документально-фактографічної і фактографічної інформації, маркетинговий відділ тощо

Мета роботи: на основі загальносистемних принципів діяльності інформаційно-технологічних підрозділів, які спеціалізуються на збиранні, обробці, зберіганні і розповсюдженні документальної, документально фактографічної і фактографічної інформації для цілей інформаційно аналітичного забезпечення сформулювати типові завдання діяльності у кожній із підсистем діяльності, визначити перелік умінь, необхідних фахівцю для виконання цих завдань.

Хід роботи: 1. Визначити перелік типових завдань діяльності, які будуть виконуватись відділом відповідно до об'єкту діяльності: документно- інформаційні ресурси – управління

інформаційною діяльністю – комунікації. Типові завдання діяльності описані функціями менеджменту (планування, організація, контроль, захист).

2. Відповідно до кожного з об'єктів діяльності та типових завдань діяльності обрати із списку (або визначити самостійно) відповідні вимоги до персоналу, визначити уміння і навички, які повинні мати працівники, які будуть працювати у відділі управління інформаційними ресурсами.

3. Заповнити таблиці (приклад в таблиці).

Таблиця 4.1.

Документно-інформаційні ресурси

Типове завдання діяльност	Уміння
-планування комплексу інформаційних ресурсів для забезпечення цілей діяльності організації - аналіз інформаційних потреб користувачів	
-організація інформаційного забезпечення діяльності організації і її співробітників; - створення умов для зберігання нормативної, довідкової та архівної інформації; - автоматизована підтримка технологічних процедур роботи з документами;	
-контроль використання інформаційних ресурсів;	
-захист інформаційних ресурсів;	

Таблиця 4.2.

Управління інформаційною діяльністю

Типове завдання діяльності	Уміння
-розробка стратегічних напрямів розвитку інформаційної діяльності організації,	
-здійснення ділових контактів підприємства із зовнішнім середовищем -здійснення окремих робіт з розробки і впровадження інформаційних систем, Веб-сайта організації та ін.;	
-управління діяльністю підрозділів, які здійснюють інформаційну діяльність, розробка посадових інструкцій співробітників	
-контроль інформаційної безпеки організації;	

Таблиця 4.3.

Комунікації

Типове завдання діяльності	Уміння
-застосування інформаційних технологій для здійснення ефективних комунікацій як всередині організації, так і з зовнішнім середовищем; -планування зовнішніх і внутрішніх комунікацій, підтримка доступу до віддалених інформаційних джерел і фондів;	
-організація комунікацій у глобальному інформаційному середовищі мережі Інтернет; -адаптація інформаційних ресурсів підприємства до розповсюдження їх через глобальні інформаційні мережі	
-комунікації упроцесах прийняття управлінських рішень; -оцінка ефективності основних комунікативних каналів	

Практична робота № 6. Тема: Планування заходів аудиту інформаційної безпеки

Хід роботи: 1. Підготовка плану заходів щодо аудиту інформаційної безпеки: а) Вибір однієї з представлених компаній. б) Формулювання вимог аудиту на підставі одного із стандартів інформаційної безпеки. в) Розробка плану заходів із зазначенням термінів, підрозділів і видів перевірок для обраної компанії.

2. Розробка підсумкового звіту за результатами аудиту: а) Підготовка найпростішої методики аналізу результатів аудиту. б) Підготовка форми аудиторського звіту із зазначенням персоналу, його заповнює, і плану проведення повторних перевірок.

3. Усі результати оформити у звіт.

Опис компаній:

1. Компанія має 5 представництв, всі п'ять в різних країнах (.com, .ua і т.д.). Має 5 представництв в кожному від 50-100 чол. Головна компанія 1000 чол в Україні. Відділ продажів у регіональному представництві, адміністративний відділ і відділ обробки даних. Напрямок діяльності компанії - транснаціональні вантажні перевезення.

2. Компанія має одне представництво в Україні, яке є компанією, купленою роком раніше, що займається розробкою програмного забезпечення. Головна компанія до 500 чол. Представництво - до 300 чол. (Різні бренди). 2 домену - 2 бренду.

3. Компанія має головний офіс зі штатом 300 чол. Займається продажем стільникових телефонів. По всій Україні 2000 - 3000 представництв - магазинів, є упр. Менеджер (локальний відділ Продажів), тарифний відділ і відділ логістики.

4. Компанія - 100 чол. Сфера діяльності аутсорсинг, послуги адміністрування різних систем на базі Майкрософт. Клієнти в більшості країн світу. Компанія забезпечує повну підтримку інфраструктури клієнта.

5. Компанія складається з 3-х філій на території України. ГО у Києві. Чисельність ГО 100 чол., у філіях 20 чол. Займається виробництвом і розробкою засобів аутентифікації. Виробництво в філіях, ГО виконує тільки адміністративні дії.

6. Компанія - холдинг з центральним офісом у м. Києві. Займається створенням та розробкою інтернет-сайтів та в неї входить ще 4 компанії, що знаходяться в 4 країнах світу. У кожній компанії до 50 осіб

5. Оцінювання знань студентів

Система оцінювання успішності здобувача вищої освіти здійснюється а 100-бальною шкалою, яка розподіляється на дві складові:

1) 60 балів – поточна складова оцінювання;

2) 40 балів – модульна або підсумкова складова оцінювання.

Усі форми контролю включено до 100-бальної шкали оцінки.

Модульну складову оцінювання організовано шляхом складання двох модульних контролів знань студентів. Перескладати модульний контроль не дозволяється.

Контрольні заходи включають також поточний контроль знань студентів. Поточний контроль є органічною частиною навчального процесу і проводиться під час лекцій та практичних занять.

Форми поточного контролю:

- перевірка підготовлених здобувачами презентацій за темами навчальної дисципліни, узгодженими з викладачем;
- перевірка домашніх завдань;
- тестова перевірка знань студентів;
- модульний контроль;
- інші форми.

6. Рекомендована література

Базова

1. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. К. : Кондор, 2004. 384 с.
2. Лодон Дж. Управление информационными системами : учебник/ Дж. Лодон, К. Лодон. 7-е изд. СПб. : Питер, 2005. 912 с.
3. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособ. для вузов. М. : Горячая линия - Телеком, 2004. 280 с.
4. Матвієнко О. Інформаційний менеджмент: аналіз предметної галузі. *Вісник Книжкової палати*. 2004. № 8. С. 13–17.
5. Матвієнко О.В. Концепція менеджменту інформаційних систем в контексті загальних проблем інформатизації суспільства. *Вісник Книжкової палати*. 2002. № 10. С. 17–20.
6. Інформаційна складова державної політики та управління : монографія / Соловйов С. Г. та ін. К., 2015. 320 с.
7. Інтеграція України в Європейський інформаційний простір: виклики та завдання. К., 2014. 212 с.

Допоміжна

8. Ярочкин В. И. Информационная безопасность : учебник. М. : Академический Проект: Фонд "Мир", 2003. 640 с.
9. Інформаційна політика в Україні: методичні рекомендації до проведення практичних занять з дисципліни / Н. В. Грицяк. К. : НАДУ, 2014. 48 с.
10. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. 2011. 78 p.
11. Swanson M. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems / M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes. 2010. 149 p.
12. Інформаційна складова державної політики та управління: монографія / Соловйов С. Г. та ін.; за заг. ред. Н. В. Грицяк. К. : К.І.С., 2015. 320 с.
13. Інтеграція України в Європейський інформаційний простір: виклики та завдання. К. : ФОП Клименко, 2014. 212 с.
14. Грицяк Н. В., Литвинова Л. В. Державне управління в умовах розвитку інформаційного суспільства : навч. посіб. /. за заг. ред. Н. В. Грицяк. К. : К.І.С., 2015. 108 с.
15. Грицяк Н. В., Литвинова Л. В.Електронна демократія : навч. посіб. / за заг. ред. Н. В. Грицяк. К. : К.І.С., 2015. 66 с.
16. Інформаційна політика в Україні: методичні рекомендації до проведення практичних занять з дисципліни / Н. В. Грицяк, А. І. Семенченко, Л. В. Литвинова, С. Г. Соловйов. К. : НАДУ, 2014. 48 с.

Інформаційні ресурси в Інтернеті

1. Верховна Рада України, законодавство України. URL: http://zakon4.rada.gov.ua/laws/a#Find (дата звернення 25.06.2018).

2. Офіційний Web-сайт Президента України. URL: http://www.president.gov.ua/.

3. Офіційний Web-сайт Кабінету Міністрів України. URL: http://www.kmu.gov.ua/ (дата звернення 25.06.2018).

4. Національна бібліотека ім. В. І. Вернадського. URL: http://www.nbuv.gov.ua/ (дата звернення 25.06.2018).

6. Наукова бібліотека Східноукраїнського національного університету імені Даля. URL: http://www.library.snu.edu.ua (дата звернення 25.06.2018).

7. Про судоустрій і статус суддів: Закон України. ВВР. 2010. № 41-42, 43, № 44-45. Ст. 529. Конституція України Розділ IV. Верховна Рада України. URL: https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-iv

8. Про Регламент Верховної Ради України: Закон України від 10 лютого 2010 року № 1861-VI. URL: https://zakon.rada.gov.ua/laws/show/1861-17.

9. Рівненська обласна універсальна наукова бібліотека (м. Рівне, пл. Короленка, 6). URL: http://libr.rv.ua/ (дата звернення 25.06.2018).

10. Рівненська централізована бібліотечна система (Київська, 44, Рівне URL: https://www.facebook.com/cbs.rivne/ (дата звернення 25.06.2018).

11. Наукова бібліотека НУВГП (м. Рівне, вул. Олекси Новака, 75). URL: http://nuwm.edu.ua/MySql/page_lib.php (дата звернення 25.06.2018).