Збройних Сил України, а також очолює Раду національної безпеки і оборони України, то на ньому лежить чи не найбільша відповідальність, як гаранта безпеки держави, у прийнятті рішень що стосується ефективності системи національної безпеки та оборони України. Особливо у теперішній час, коли відбувається загроза безпеці України з боку Російської Федерації та її сателітів у формі терористичних організацій на Донбасі – ДНР та ЛНР.

ЛІТЕРАТУРА:

1. Державна безпека [Електронний ресурс]. – режим доступу http: // uk.wikipedia.org/wiki / Державна_безпека.
2. Закон України «Про основи національної безпеки України» [Електронний ресурс]. – режим доступу http: // zakon2.rada.gov.ua/laws/show/964-15.
3. Закон України «Про Раду національної безпеки і оборони України» [Електронний ресурс]. – режим доступу http: // zakon4.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80.
4. Конституція України[Електронний ресурс]. – режим доступу http: // zakon2.rada.gov.ua/laws/show/254к/96-вр.
5. Указ Президента України «Про стратегію національної безпеки України» [Електронний ресурс]. – режим доступу http: // zakon4.rada.gov.ua/laws/show/105/2007.

УДК 351.813.12

Лариса Горяна
Лілія Нападовська
Анатолій Пашков

СУЧАСНИЙ СТАН ТА ВИРІШЕННЯ ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті розглянуто питання визначення пріоритетних завдань забезпечення інформаційної безпеки. Окреслено рівні інформаційної безпеки, проаналізовано її складові на прикладі досвіду США, ЄС та Азії.

Ключові слова: *інформаційна безпека, інформаційна війна, інформаційно-комунікаційні технології, тероризм, кіберзагроза, захист.*

В статье рассматриваются вопросы определения приоритетных задач обеспечения информационной безопасности. Намечены уровни информационной безопасности, проанализированы ее структурные части на примере опыта США, ЕС и Азии.

Ключевые слова: *информационная безопасность, информационная война, информационно-комуникационные технологи, терроризм, киберугроза, защита.*

The article deals with the determination of the priority tasks of information security. It describes the level of information security, its components are analyzed on the example of the U.S., EU and Asia.

Keywords: *information security, information warfare, information and communication technologies, terrorism, cyber threats, security.*

Постановка проблеми. У сучасних умовах економічної, екологічної та інформаційної кризи, зростання соціальної напруги у суспільстві та політичної дестабілізації виникають певні причини, які підштовхують людей на різні прояви власної незгоди з політикою влади та діяльністю окремих суб`єктів господарювання. Ми стаємо свідками проведення як законних акцій соціального протесту (зокрема, руху «Проти всіх»), так і неконтрольованих державними інституціями протизаконних дій. Особливу увагу привернула безпосередньо проблема диференціації тих правопорушень, які можуть бути вчинені проти інформаційної безпеки [4, с. 57].

Система забезпечення інформаційної безпеки України ґрунтується на національних інтересах, формується з урахуванням реальних загроз, небезпек і викликів безпеці особистості, суспільства, держави та функціонує у правовому полі, визначеному Конституцією України, законами України і розпорядженнями Президента України,

рішеннями Ради національної безпеки і оборони України, постановами і розпорядженнями Верховної Ради України та Кабінету Міністрів України і державними програмами у цій галузі [5, с. 99].

На думку авторів, сучасними поширеними посяганнями на інформаційну безпеку були і залишаються, незалежно від різних чинників (політичних, економічних, екологічних, релігійних, мовних, міжетнічних та ін.) блокування транспортних комунікацій, а також захоплення транспортного підприємства (ст. 279 Кримінального кодексу України), групове порушення громадського порядку (ст. 293 КК України), масові заворушення (ст. 294 КК України), захоплення державних або громадських будівель чи споруд (ст. 341 КК України).

Такі протиправні дії не завжди визнаються злочинними. Пригадаймо сумнозвісні вибори Президента України 2004 р., коли групове порушення громадського порядку не отримало певної правової оцінки. Такі дії були оцінені як крайня необхідність, зважаючи на перемогу «помаранчевої революції». Проте програми «помаранчевої команди», напевно, змінив би оцінку влади до таких подій чого не сталося. Тому заручниками у таких конфліктах можуть ставати звичайні «прості» громадяни, бо, як відомо, керівників політичних партій (рухів) і народних депутатів України практично важко (як засвідчує судова практика – неможливо) притягнути до кримінальної відповідальності.

Разом з тим, стабільне функціонування держави, зростання економічного потенціалу будь-якого підприємства в умовах розвитку інформаційних відносин багато у чому залежать від наявності надійної системи інформаційної безпеки.

Зважаючи на висловлене дослідження передового досвіду взаємодії державного та недержавного секторів США, ЄС та КНР у сфері інформаційної безпеки може бути використаний для розроблення рекомендацій щодо удосконалення системи забезпечення національної безпеки України.

Аналіз останніх досліджень і публікацій. Президент США Барак Обама задекларував, що кіберзагроза є однією з найбільш серйозних економічних і національних проблем безпеки, що стоять перед нацією [8, с. 1].

Учені порівнюють використання інформаційно-комунікаційних технологій із злочинними намірами з зброєю масового ураження [10, с. 1].

Перші 30 років після утворення нового Китаю вважалося, що основними проблемами світового характеру є війна і революція, тому концепція безпеки була сконцентрована на оборонній та політичній безпеці, тобто на територіальній цілісності й суверенітету країни, а також на зміцненні державної влади. Таку концепцію називають традиційною.

У даний період Китай, не випускаючи з уваги традиційних загроз безпеці акцентує увагу й на нетрадиційних загрозах у таких галузях, як економіка, інформатика, енергетика, продовольство, охорона здоров`я та на боротьбі з тероризмом. Таким чином, на сьогоднішній день Китай веде боротьбу маючи власну національну військову стратегію і такий напрямок, як інформаційна війна (ІВ) та пропонує можливість вигравати війни без традиційного зіткнення озброєнь [7, с. 89].

Як наслідок, за останні роки Китай продемонстрував інтенсивне захоплення інформаційною війною. Потенційна здатність Китаю до посилення інформаційної революції, що супроводжується своїм поступовим підвищенням як головної військової сили, привела багатьох спостерігачів до міркування про те, чи не вдалося Китаю стати одним з глобальних лідерів ІВ. Суперечливим є й те, що тільки Сполучені Штати й Росія складають конкуренцію Китаю в аналітичній розробці ІВ.

З огляду на висловлене **метою написання статті** є аналіз сучасного стану інформаційної безпеки в Україні та у світі й обґрунтування основних завдань і рівнів адміністративно-правового забезпечення інформаційної безпеки діяльності людини, суспільства та держави з

урахуванням сучасних викликів та загроз.

Виклад основного матеріалу. Як загальнонаукова категорія безпеку можна визначити тоді, коли вона здатна протистояти впливу зовнішніх та внутрішніх загроз, а також у той час, коли функціонування цієї системи не створює загрози для складових цієї системи і зовнішнього середовища.

Разом з тим, стабільне функціонування і зростання економічного потенціалу будь-якого підприємства в умовах розвитку інформаційних відносин багато у чому залежить від наявності надійної системи інформаційної безпеки. Свого часу американський соціолог Даніель Белл у своєму дослідженні зазначав: "постіндустріальне суспільство базується на послугах. Тому воно становить собою гру між людьми. Головне значення мають вже не мускульна сила і не енергія, а інформація…" [1, с. 328].

Про важливість інформаційної безпеки у світі існують афоризми: "попереджений значить озброєний", "хто володіє інформацією, той володіє всім".

Нажаль, ситуація в Україні сьогодні ускладнена тим, що українські інформаційні технології значною мірою відстають від світових стандартів слабко розвинена вітчизняна індустрія засобів інформатизації, телекомунікацій і зв`язку.

Це змушує органи державної влади при створенні інформаційних систем закуповувати імпортну техніку і залучати іноземні компанії. У результаті підвищується вирогідність несанкціонованого доступу до оброблюваної інформації і зростає залежність від іноземних виробників комп`ютерної техніки.

Проте однією із обов`язкових вимог до країн-кандидатів на приєднання до ЄС є створення умов для побудови інформаційного суспільства, основними стратегічними цілями розвитку якого є [2, с. 26]:

– прискорення розроблення та впровадження новітніх вітчизняних конкурентоспроможних інформаційно-комунікаційних технологій в усі сфери суспільного життя,

зокрема у інформаційну безпеку і економіку України та в діяльність органів державної влади, органів місцевого самоврядування;

– державна підтримка нових електроних секторів економіки (торгівлі, надання фінансових і банківських послуг, тощо);

– створення загальнодержавних інформаційних систем, в першу чергу у сферах безпеки, охорони здоров`я, освіти, науки, культури і охорони довкілля;

– захист інформаційних прав громадян та мінімізації ризику "інформаційні нерівності";

– удосконалення законодавства із регулювання інформаційних відносин враховуючи передовий світовий досвід.

Уперше у США в 1906 р. був прийнятий закон про захист інформації, на сьогодні, вже майже 500 законодавчих актів, що регулюють питання захисту інформаційної безпеки (ІБ), протидії комп`ютерним злочинам.

Політика ІБ США формується на 2 рівнях [9, с. 130]. *На процедурному рівні* (табл.1) визначаються безпосередньо заходи щодо забезпечення ІБ суб`єкта господарювання. До них вони відносять управління персоналом, фізичний захист і планування роботи. *На програмно-технічному рівні* здійснюється захист устаткування програмних засобів та інформаційних ресурсів. Реалізується це за допомогою сервісів безпеки: 1) ідентифікація та аутентифікація; 2) розмежування доступу; 3) протоколювання й аудит; 4) шифрування; 5) забезпечення цілісності; 6) екранування; 7) забезпечення доступності; 8) забезпечення стійкості.

Таблиця 1

Заходи щодо забезпечення ІБ суб`єкта господарювання на процедурному рівні

Управління	Фізичний знос	Планування
Вимоги	Охоронно-пожарна система	Протидія
Посадові інструкції	Захист території	Відновлення робіт
Навчання	Системи контролю та доступу	

Заслуговує на увагу ІБ ЄС на прикладі Франції. Базовим нормативним актом, в якому визначаються стратегічні напрями державної політики Франції у сфері забезпечення безпеки є Біла книга оборони та національної безпеки від 2008 р. [6, с. 70], в якій серед найбільш ймовірних загроз території Франції та Європейської спільноти (тероризм, використання балістичних ракет, злочинність, ризики природного характеру та ускладнення епідеміологічної ситуації у великих містах прихована імміграція) названі: масштабні атаки на інформаційні системи, шпіонаж та стратегічний вплив.

Основними шляхами протидії цим загрозам у документі визначено:

– взаємодію у питаннях протидії атакам на інформаційні системи, насамперед у межах країн-членів ЄС;

– проведення як відкритих так і прихованих активних заходів протидії проявам агресії в інформаційних мережах;

– підготовка кібервійськ на професійній основі.

Закон від 19 травня 2005 року №2005-493 у Франції ратифікував Конвенцію Ради Європи, "Про кібер-злочинність" відповідно до якої комп`ютерні злочини класифікують за 2 напрямами:

1) інформаційні технології як засоби виконання незаконних дій (продажу контрфактних товарів, заборонених ліків, сутенерства, дитячої порнографії, незаконних фінансових махінацій, тощо);

2) інформація як об`єкт злочину (несанкціонований доступ, порушення цілісності даних, махінації в платіжних системах та ін.).

Принциповою є державна політика Франції щодо захисту національної самобутності у медіа просторі: 60% телерадіоефіру має заповнюватися власною аудіовізуальною продукцією, причому 40% із неї має бути франкомовною та трансльованою у пройм-тайм.

Стержнем Білої книги 1972 р. було "стримування", 1994 р. – "проектування сили", у документі 2008 р. – "знання

й прогнозування", що становить нову стратегічну функцію, пріоритетне завдання у сфері безпеки та оборони.

У Білій книзі безпеки і оборони визначені 4 основні завдання на забезпечення ІБ:

– бути світовим лідером у сфері кіберзахисту – належати до країн, які домінують у цій сфері;

– гарантувати свободу рішень Франції у питаннях захисту інформаційного суверенітету – забезпечити прийняття рішень органами влади на підставі неупередженої захищеної інформації;

– зміцнити кібербезпеку національної критичної інфраструктури;

– забезпечити безпеку громадян та бізнесу у кіберпросторі.

Критерії віднесення інформації до секретної та особливо секретної розробляються урядом і затверджуються прем`єр-міністром.

США, Європа та країни з економікою, що швидко розвиваються, такі як Китай вкладають все більше грошей у дослідження у сфері високих технологій та інформаційної безпеки. На сьогодні Китай випередив Японію за обсягами свого Валового національного продукту (весна 2010 р.). Обсяг експорту Китаю до країн ЄС перевищив відповідний показник США та ін. На думку авторів, головними причинами цього явища стали освітні зміни в Китаї.

За даними ЮНЕСКО в Китаї у 1999 р. навчалося 6,3 млн. студентів, а 2005-2006 н.р. вже 23,4 млн. студентів. Високий рівень до університетської підготовки пояснюється комп`ютеризацією класів у школі та високою працею школярів Китаю, які приходять до школи до 6.30 ранку, а йдуть об 8– 9.00 годині вечора [3, с. 26].

Саме якісна освіта Китаю дозволяє усвідомити проблеми значення інформаційної безпеки, безпеки харчових продуктів, охорони здоров`я і боротьби із сепаратизмом і тероризмом. А наявність сьогодні протиріч і конфліктів між країнами додатково пояснює сильний інтерес Китаю до інформаційних війн (ІВ) наступними 3 факторами:

по-перше, Китай зрозумів значення високої технології та зростаючи владу інформації в еру глобалізації та взаємозалежності; *по-друге,* Китай став прагнути головним політичним і економічним гравцем у глобальному співтоваристві; *по-третє*, багато китайців вірять, що ІВ одна з небагатьох технологічних арен, де боротьба за перевагу великих держав залишається незавершеною. Китай сподівається перескочити через покоління застарілих технологій.

Висновки. Основними завданнями адміністративно-правового забезпечення інформаційної діяльності будь-якого суб`єкта господарювання і національної безпеки, на нашу думку, є створення стабільної ефективної торгівельної і виробничої діяльності усіх підрозділів, захист від втрат, крадіжок, створення і зниження конфіденційної інформації та комерційної таємниці, розкрадання фінансових коштів, попередження загроз. Система інформаційної безпеки потрібна також для підвищення якості послуг, що надаються і гарантії безпеки майнових прав та інтересів клієнтів.

Для досягнення зазначених цілей, у першу чергу, потрібно:

– категорування інформації на конфенденційну та комерційну таємницю;

– прогнозування та своєчасне виявлення загроз ІБ, причин і умов, які є сприятливими щодо нанесення державного, військового, фінансового, матеріального і морального збитку;

– створення механізму і умов для ефективного реагування на загрози ІБ, на основі економічних, правових, організаційних та технічних засобів.

Європейська інтеграція України передбачає залучення нашої держави до процесу побудови "Концепції" єдиного європейського інформаційного простору і подолання суттєвого дисбалансу між інформаційними просторами України та ЄС, яка б встановлювала системний підхід до проблем національної безпеки і інформаційних ресурсів та враховувала б сучасний європейський досвід.

Подальші дослідження в цій сфері мають бути спрямовані на побудову Концепції національної безпеки України у відповідності до ЄС.

ЛІТЕРАТУРА:

1. Белл Д. Грядущее постиндустриальное общество. Опыт социального пронозирования / Д. Белл пер. с англ. – М. : Академия. – 2006. – 788 с.
2. Довгань О.Д. Європейська інтеграція України як чинник удосконалення вітчизняного інформаційного законодавства / О.Д. Довгань, О.М. Солодка // Інформаційна безпека людини, суспільства, держави. – К. : Національна академія СБУ, 2013. – №1. – С.25-29.
3. Європа, США і Азія : суперництво в галузі знань // Сучасна освіта. – К. : Основа, 2012. – №5. – С. 26-27.
4. Кузнецов В.В. Особливості сучасних посягань на національну безпеку/ Бізнес та безпека: концептуальні засади та практичні аспекти. Зб. наук. праць. – К. : Європейський ун-т, 2010. – С. 57-60.
5. Ленков С.В. Формалізація слабкоструктурованих задач при вирішенні практичних задач забезпечення національної безпеки / С.В. Ленков, Я.Я. Винярський, О.В. Дергильова. – Луганськ : Східноукраїнський нац. ун-т, 2013. – №2(10). – С. 99-102.
6. Панченко В.М. Сучасний стан нормативно-правового забезпечення Франції у галузі інформаційної безпеки / В.М. Панченко // Інформаційна безпека людини, суспільства, держави. – К. : Нац. академія СБУ, 2012. – №2. – С. 70-75.
7. Самаріна М.В. Досвід організації інформаційної безпеки КНР / Бізнес та безпека: концептуальні засади та практичні аспекти / М.В. Самаріна // Зб. наук. праць. – К. : Європейський ун-т, 2010. – С.89-90.
8. Cybersecurity [Електронний ресурс]. Режим доступу: http.www.whitehouse.gov/administration/eop/nsc/cyber security.
9. Чистоклетов Л.Г. Завдання та рівні забезпечення безпеки діяльності суб`єктів господарювання в інформаційній

сфері / Л.Г. Чистоклетов // Інформаційна безпека людини, суспільства, держави. – К. : Нац. академія СБУ, 2013. – №1(11). – С.126-132.
10. Шерстюк В. Кибертерроризм приравняли к оружию массового поражения [Електронний ресурс]. Режим доступу: www.interface.ru/nome.asp.artid.

УДК 613.959: [37:001.895]

Юрій Гріненко

БЕЗПЕЧНІ УМОВИ ЖИТТЄДІЯЛЬНОСТІ ШКОЛЯРІВ ПІД ЧАС УПРОВАДЖЕННЯ ПЕДАГОГІЧНИХ ІННОВАЦІЙ

У статті проаналізовано безпечні умови життєдіяльності та гігієнічні принципи збереження здоров'я школярів в умовах упровадження педагогічних технологій та освітніх інновацій; запропоновано найбільш поширені здоров'язбережувальні педагогічні технології.

Ключові слова: *школяр, здоров'я, безпека життєдіяльності, педагогічні технології, здоров'язбережувальні технології.*

В статье проанализированы безопасные условия жизнедеятельности и гигиенические принципы сохранения здоровья школьников в условиях внедрения педагогических технологий и образовательных инноваций; предложено наиболее распространенные здоровьясохраняющие педагогические технологии.

Ключевые слова: *школьник, здоровье, безопасность жизнедеятельности, педагогические технологии, здоровьясохраняющая технологии.*

The article analyzes the safe conditions of pupil's vital activity and hygiene of children's health during the pedagogic technology adaptation. We have suggested the most wide-spread pedagogical technologies, which are safe for the health.

Keywords: *pupil, health, vital activity, pedagogical technologies, safe for health technologies.*

Постановка проблеми. Реформування сучасної освіти вимагає створення та використання інноваційних педагогічних технологій, які спрямовуються на забезпечення умов для самореалізації особистості. Водночас розв'язання нових освітніх завдань не завжди супроводжується відповідною організацією охорони і збереження здоров'я школярів. Саме тому зусилля педагогів повинні бути спрямовані на створення сприятливих умов життєдіяльності школярів під час організації навчально-виховного процесу.

Аналіз останніх досліджень і публікацій. Результати наукових досліджень свідчать, що впровадження нових форм навчання може мати негативний вплив на здоров'я школярів унаслідок впливу цілої низки чинників. До таких чинників, дослідники В.І. Бобрицька [2], Н.І. Коцур [5] відносять: інтенсифікацію навчальної діяльності; зміни режиму дня; тривалу психоемоційну напругу, розвиток «шкільного стресу»; порушення санітарно-гігієнічних та протиепідемічних нормативів внутрішньошкільного середовища; впровадження нових форм без відповідного медико-психолого-педагогічного супроводу й оцінки ефективності.

Метою нашого дослідження було з'ясування безпечних умов життєдіяльності та здоров'я школярів під час упровадження освітніх інновацій.

У процесі реалізації поставленої мети було поставлено такі ***завдання:***

– зробити огляд джерел і літератури стосовно аналізу безпечних умов життєдіяльності і здоров'я школярів під час упровадження інноваційних педагогічних технологій;

– проаналізувати найбільш поширені здоров'язбережувальні педагогічні технології.

Виклад основного матеріалу. Дослідження вчених-гігієністів останніх років (Бардов В.Г., Берзінь В.І., Даниленко І.Л., Кучма І.Р., Сергета І.В., Полька Н.С. та ін.) дали змогу обґрунтувати гігієнічні принципи збереження