ability of eavesdroppers' detection, eavesdroppers' amount of information.

Василіу Євген Вікторович, доктор технічних наук, доцент, директор навчально-наукового інституту радіо, телебачення та електроніки Одеської національної академії зв'язку ім. О.С. Попова.
E-mail: vasiliu@ua.fm
Василиу Евгений Викторович, доктор технических наук, доцент, директор учебно-научного института радио, телевидения, электроники Одесской национальной академии связи им. А.С. Попова.
Vasiliu Yevhen, Doctor of Science in Eng., Full Professor, Director of Educational and research institute of radio, television, electronics Odessa national academy of telecommunications named after O.S.Popov.
Ніколаєнко Сергій Вадимович, викладач Одеської національної академії телекомунікацій ім. Попова О.С.
E-mail: serezhanik@gmail.com
Николаенко Сергей Вадимович, преподаватель Одесской национальной академии связи им. А.С. Попова.
Nikolayenko Sergiy, Lecturer at IT Dept, Odessa National Academy of Telecommunications named after O.S. Popov.

УДК 004.056; 681.58

ДІЛОВІ ІГРИ ЯК МЕТОД ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Наталія Шиліна, Юрій Копитін

Забезпечення належного рівня інформаційної безпеки напряму залежить від якісної професійної підготовки майбутніх фахівців, рівня впровадження та використання інноваційних педагогічних, інформаційно-комунікаційних технологій та формування інформаційної культури. Проаналізований сучасний стан підготовки фахівців з інформаційної безпеки свідчить, що поточні вимоги до вмінь та навичок студентів не відповідають тим, які необхідні для побудови ефективної системи управління інформаційною безпекою організації. У роботі розкрито методику проведення ділових ігор для підготовки фахівців з інформаційної безпеки. Описаний метод підготовки фахівців дозволить студентам краще осмислити матеріал, розвинути свої творчі здібності в розв'язанні проблеми захисту інформації, розбиратися в тих чи інших питаннях інформаційної безпеки та вчитися працювати в колективі. Ділові ігри допоможуть забезпечити майбутніх фахівців з інформаційної безпеки необхідними теоретичними знаннями та практичними навиками у сфері сучасних методів та засобів захисту інформації.

***Ключові слова**: інформаційна безпека; модель вищої професійної освіти; технічний захист; ділові ігри; професійна підготовка.*

1. ВСТУП. Стрімкі темпи впровадження нових інноваційних та інформаційно-комунікаційних технологій (ІКТ), зростання обсягів цифрової інформації і підвищення її значимості несуть у собі ризики, що можуть призвести до порушення цілісності, конфіденційності, доступності інформації та заподіяння шкоди.

Саме тому власники, розпорядники і користувачі інформаційних ресурсів повинні розуміти, що надійний захист інформації та гарантоване покриття ризиків можливі тільки за умови забезпечення належного рівня інформаційної безпеки (ІБ), яка є невід'ємною складовою кожної зі сфер національної безпеки і водночас важливою самостійною сферою забезпечення національної безпеки держави [1].

Забезпечення належного рівня ІБ напряму залежить від якісної професійної підготовки майбутніх фахівців, рівня впровадження та використання інноваційних педагогічних, інформаційно-комунікаційних технологій та формування інформаційної культури. В сучасних умовах переходу від когнітивної до компетентнісної моделі побудови змісту освіти це особливо важливо для України, яка модернізується як європейська держава та інтегрується в світове інформаційне співтовариство.

У зв'язку з цим зростає потреба у кваліфікованих фахівцях у галузі інформації безпеки, оскільки рівень захищеності інформації безпосередньо залежить від рівня підготовки кадрів у національній системі освіти.

Проблема підготовки національних кадрів з інформаційної безпеки широко обговорюються у наукових виданнях, засобах масової інформації, в мережі Інтернет, на науково-практичних конференціях, семінарах, круглих столах.

Різним аспектам підготовки фахівців з інформаційної безпеки та захисту інформації присвячені публікації Томашевського О.В., Хорошко В.О., Бєлякова К.І., Голубенка О.Л., Петрова О.С., Маклакова Г.Ю., Коляди М.Г. та інших. В даних публікаціях розкрито стан, проблеми, особливості, організаційні, науково-методологічні аспекти та теоретико-методичні основи підготовки фахівців, а також перспективи такої підготовки. Однак впровадження у навчальний процес новітніх технологій, форм і методів активного навчання фахівців з інформаційної безпеки розкрито недостатньо.

У зв'язку з цим, *метою статті* є презентація ділових ігор як методу підготовки фахівців з інформаційної безпеки, що спонукатиме студентів до творчого та критичного мислення і реалізації своїх здібностей, дозволить глибше пізнати предмет, а також отримати певні практичні навички.

2. ОПИС ПРОБЛЕМИ. На сьогодні однією з пріоритетних задач сучасної системи освіти є пошук моделей вищої професійної освіти, які адекватні сучасному типу культури і відповідають новому етапу розвитку інформаційного суспільства. У вищих навчальних закладах (ВНЗ) актуалізуються нові вимоги до професійної підготовки майбутніх фахівців у сфері ІБ.

Актуальність даної тематики розкрита в концепції технічного захисту [2], де зазначено, що одним з першочергових заходів щодо реалізації державної політики у сфері технічного захисту інформації (ТЗІ) є розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

До основних чинників, які визначають актуальність зазначеної проблеми, також можна віднести постійно зростаючу кількість інформаційних загроз і ризиків, низький рівень забезпеченості інформаційної безпеки в організаціях, недостатню методичну базу та відсутність комплексних ґрунтовних досліджень з означеної проблеми.

В даний час у галузі освіти та інформаційної безпеки спостерігаються такі основні проблеми:

- не сформована загальна концепція підготовки фахівців у сфері забезпечення ІБ з урахуванням вимог міжнародних стандартів;
- відсутня цілісна концепція теорії забезпечення ІБ та методології захисту інформації, що заважає формуванню професійної компетентності майбутніх спеціалістів у сфері забезпечення ІБ;
- відсутня цілісна термінологічна система, яка б сформувала єдиний термінологічний апарат у сфері ІБ;
- не в усіх ВНЗ у повному обсязі оновлено програми із спеціальних дисциплін;
- недостатнє фінансування та застаріла матеріально-технічна база;
- надмірно широке впровадження програмних продуктів іноземного виробництва;
- невідповідність переліку спеціальностей, за якими ведеться навчання у ВНЗ, реальним професіям, які існують в індустрії інформаційних технологій;
- основна увага приділяється використанню різних технологічних рішень на програмному та апаратному рівнях, без урахування людського чинника;
- розвиток законодавства у сфері ІБ помітно відстає від сучасного розвитку технологій безпеки;
- багато уваги в ВНЗ приділяється теоретичним питанням, які на практиці не застосовуються;
- не вирішена проблема підтвердження дипломів, отриманих за кордоном;
- не розуміння керівниками організацій важливості гарантування інформаційної безпеки для успішного ведення бізнесу;
- дефіцит науково-педагогічних кадрів та кваліфікованих фахівців в галузі інформаційної безпеки;
- недостатня увага до інцидентів інформаційної безпеки.

Основним недоліком сучасної освіти у ВНЗ є недостатня практична діяльність майбутніх фахівців з урахуванням вимог ринкових відносин.

Нині підготовка фахівців з інформаційної безпеки спрямована в основному на інженерно-технічні заходи та програмно-апаратні засоби захисту інформації. В процесі навчання студенти отримують сугубо технічні навички, але не мають в повному обсязі уявлення про лідерство, управління ресурсами, персоналом, бізнес процесами, ризиками. Вимоги до вмінь та навичок абсолютно не відповідають тим, які необхідні для ефективного управління інформаційною безпекою, а також побудови системи захисту інформації організації.

Згідно Постанови Кабінету міністрів України № 787 від 27.08.2010 р. "Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-

кваліфікаційними рівнями спеціаліста і магістра" [3] та наказу Міністерства освіти і науки України № 1067 від 09.11.2010 р. [4] з 2011/2012 навчального року вводиться в дію перелік спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах України за освітньо-кваліфікаційними рівнями спеціаліста і магістра.

Підготовка фахівців з інформаційної безпеки у вищих навчальних закладах України здійснюється за спеціальностями наведеними в табл. 1.

Напрями підготовки фахівців з інформаційної безпеки Таблиця 1

Найменування галузі знань	**Напрям підготовки**	**Код напряму підготовки**	**Найменування спеціальності**	**Код спеціальності**
Інформаційна безпека	Безпека інформаційних і комунікаційних систем	6.170101	Безпека інформаційних і комунікаційних систем	7.17010101 8.17010101
			Безпека державних інформаційних ресурсів	7.17010102 8.17010102
	Системи технічного захисту інформації	6.170102	Системи технічного захисту інформації, автоматизація її обробки	7.17010201 8.17010201
	Управління інформаційною безпекою	6.170103	Управління інформаційною безпекою	7.17010301 8.17010301
			Адміністративний менеджмент у сфері захисту інформації	7.17010302 8.17010302

Перелік державних вищих навчальних закладів, ліцензованих за напрямами підготовки 1601, 1701 в галузі знань «Інформаційна безпека» чітко визначений [5].

3. ВПЛИВ РІВНЯ ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВЕНЬ РИЗИКІВ. Ризики для організації, пов'язані з різними впливами на її інформаційну інфраструктуру, є невід'ємною частиною процесу управління безперервністю бізнесу. Вимірювання ризиків (risk estimation) є найбільш складним етапом в процесі управління ризиками інформаційної безпеки.

Рівень ризику (очікуваний річний збиток) [6] розраховується за формулою:

$$ALE = ARO \cdot SLE, \quad (1)$$

де ARO – річна частота події, інакше кажучи імовірність виникнення збитків;

SLE – очікуваний одиничний збиток, тобто вартість збитку від однієї успішної атаки, яка розраховується за формулою:

$$SLE = AV \cdot EE, \quad (2)$$

де AV – вартість активу;

EE – фактор впливу, тобто розмір збитків або впливу на значення активу (від 0 до 100%), тобто частина значення, яку актив втратив в результаті негативної події.

Розглянемо більш детально імовірність виникнення збитків (ARO). На думку авторів на частоту події впливає величезна кількість чинників серед яких: технічні (впроваджені засоби захисту), правові (наявність нормативних документів, в яких значиться відповідальність порушника за скоєний інцидент), організаційні (налагоджений процес правління інформаційною безпекою), освітні (рівень знань співробітників з питань безпеки), економічні (цінність інформації), соціальні (наявність невдоволених осіб) тощо.

Рівень підготовки фахівців, тобто освітній чинник, прямо пропорційно впливає на частоту появи негативної події. Така сама залежність характерна й іншим чинникам. Визначення математичної залежності впливу кожного з чинників на імовірність виникнення збитків є темою наступного дослідження.

4. ДІЛОВІ ІГРИ В ПІДГОТОВЦІ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. В умовах ринкової економіки та конкурентного середовища основними вимогами роботодавців є:

- якісна професійна підготовка студентів;
- уміння та навички ділового спілкування, в тому числі роботи в команді;
- готовність до безперервної самоосвіти і модернізації професійної кваліфікації;
- здатність знаходити та використовувати інформацію з різних джерел;
- уміння діяти і приймати відповідальні рішення в нестандартних і невизначених ситуаціях.

Тобто ключовим тут є той факт, що роботодавцю недостатньо наявності тільки теоретичних знань. На сьогоднішній день випускнику важливо мати культурні, мовні, комунікативні навички, а також вміння працювати в команді.

Так, навіть ті випускники ВНЗ, які отримали якісні спеціалізовані знання, як правило, зовсім не вміють працювати в системі, проектах, де потрібні навички командної, групової взаємодії, управління часом і проектом як таким [7]. Розвиток творчого потенціалу та інтелектуальних здібностей потребує перегляду мети освіти: вона має бути більш динамічною, пов`язаною з ініціативною поведінкою суб`єктів навчання.

На думку авторів найбільш оптимальним шляхом підвищення рівня знань студентів є самостійна робота студентів, яка, згідно статті 43 ЗУ «Про вищу освіту»[8], є однією з форм реалізації навчального процесу. Одним із варіантів ефективної реалізації самостійної роботи студентів є використання методів активного навчання (МАН).

Методи активного навчання – це, власне, способи активізації навчально-пізнавальної діяльності студентів, які спонукають їх до активної мисленнєвої та практичної діяльності в процесі оволодіння матеріалом, за умови активності не тільки викладача, але й самих студентів. [9].

Значний вклад у становлення та розвиток ігрового методу зробили праці Буркова В.Н., Єфимова В.М., Комарова В.Ф., Жукова Р.Ф., Платова В.Я., Хачатурян А.П. та ін.[10]

Ігрові методи поділяють на:
- ділові ігри;
- дидактичні або навчальні ігри;
- ігрові ситуації;
- ігрові прийоми;
- тренінги в активному режимі [11].

Детальний опис ігрових методів подано у різних джерелах. В нашій статті ми зупинимось на ділових іграх, які охоплюють усі аспекти активізації діяльності студента.

Ділова гра – це форма відтворення предметного та соціального змісту професійної діяльності, моделювання системи відносин, характерних до даного виду практики [12].

Тобто можна сказати, що ділова гра має на меті імітацію спільної діяльності людей, імітацію прийняття управлінських рішень в різних виробничих ситуаціях, іноді досить нестандартних, у режимі інтерактивного діалогу.

Ємельянов С.В., Бурков Н.В., Івановський А.Г. визначають ділову гру як модель взаємодії людей в процесі досягнення деяких цілей економічного, політичного або престижного характеру [13]. У більш широкому сенсі ділова гра виступає як модель процесу прийняття рішення [14].

Ділова гра суттєво активізує навчально-пізнавальну діяльність студентів, оскільки їй притаманні такі особливості:

1) системне представлення змісту навчального матеріалу в імітаційній моделі;
2) відтворення структури і функціональних ланок майбутньої професійної діяльності в ігровій навчальній моделі;
3) формування у студентів потреби у знаннях і їхньому практичному застосуванні, що забезпечує усвідомленість навчання, особистісну активність, перехід від пізнавальної мотивації до професійної;
4) комплексний навчально-виховний вплив на особистісне і професійне становлення студентів;
5) забезпечення переходу від організації та регуляції діяльності викладачем до саморегуляції та самоорганізації діяльності самими студентами [15].

На нашу думку саме ці особливості ділової гри дозволять студентам отримати цілісне уявлення про майбутню роботу, виробити предметно-професійний та соціальний досвід, у тому числі досвід прийняття індивідуальних і колективних рішень, розкрити професійне мислення, а також активізувати навчальну діяльність, формувати пізнавальну мотивацію.

Важливим, на думку авторів, є максимальне наближення ділової гри до практичної діяльності, тобто дії студентів повинні бути максимально наближеними до дій співробітників організації та виходити з певної ситуації. У літературі виділяють кілька типів конкретних ситуацій (кейсів) [16]. З точки зору результату гри вони поділяються на проблемні і проектні. У проблемних ситуаціях результатом дії є визначення та формулювання основної проблеми та, головне, оцінка складності її вирішення.

За джерелами інформації кейси поділяються на:
- ті, які описують реальні ситуації, почерпнуті з практичної роботи;
- штучно структуровані в навчальних цілях або для опрацювання гіпотетичних проблем, які можуть виникнути перед організацією. За допомогою методу конкретної ситуації виробляються вміння і навички самостійної роботи, наприклад, такі як індивідуальне та групове прийняття рішення щодо поставлених завдань. Такого роду здібності вкрай необхідні для самостійної діяльності фахівця, оскільки йому безперервно доводиться приймати нестандартні рішення, викликані змінами стану справ. Метод конкретної ситуації розвиває у студентів широту і гнучкість мислення,

допомагає навчити їх вмінню раціонально використовувати інформацію, відчувати її, самостійно аналізувати факти, критично розглядати різні точки зору, обговорювати і захищати власну позицію, бути готовим до застосування різних засобів і методів, знаходити оптимальне вирішення питань [17].

Слід зазначити, що саме по собі використання ділових ігор не гарантує підвищення ефективності навчальної діяльності студентів. Лише за певних педагогічних умов застосування ділових ігор може сприяти активізації пізнавальної діяльності майбутніх фахівців з інформаційної безпеки. У зв'язку з чим опишемо методику підготовки ділових ігор для майбутніх фахівців інформаційної безпеки.

Першим кроком є визначення теми, завдання та дидактичної мети гри.

У темі, зазвичай, відображаються характер, масштаби та обставини подій на об'єкті інформаційної діяльності. Наприклад, темами можуть бути: дослідження методів пошуку уразливості інформаційної безпеки, вимірювання економічної ефективності системи захисту інформації банківської установи, створення технічного завдання на впровадження комплексу технічного захисту інформації в органі місцевого самоврядування тощо.

Завдання повинно включати зміст заходів, які слід виконати студентам для отримання певних теоретичних знань та практичних навичок. Завдання має бути тісно пов'язане з тематикою гри. Наприклад, у випадку обрання теми, яка стосується створення комплексу технічного захисту інформації, необхідно чітко описати об'єкт, на якому створюється комплекс, умови його функціонування, вплив внутрішніх та зовнішніх чинників, необхідний рівень захищеності, який слід досягти тощо.

Метою гри може бути: демонстрація належного виконання конкретного завдання; показ оптимального зразка прийняття рішення у певній ситуації тощо. Основним завданням мети є відповідь на питання для чого студентам потрібна дана гра.

Для досягнення поставленої навчальної мети на етапі розробки ділової гри слід орієнтуватись на такі психолого-педагогічні принципи:

- принцип імітаційного моделювання ситуації;
- принцип проблемності змісту гри і її розгортання;
- принцип рольової взаємодії в спільній діяльності;
- принцип діалогічного спілкування;
- принцип двоплановості ігрової навчальної діяльності [18].

Проведення психологічного аналізу поведінки учасників гри дозволить закласти успішну реалізацію наступних кроків.

Реалізація даного кроку здійснюється шляхом:

а) виділення структурних елементів майбутньої професійної діяльності студентів. У фахівців інформаційної безпеки можливі такі основні види професійної діяльності: науково-дослідна; проектна; контрольно-аналітична; організаційно-управлінська; експлуатаційна;

б) з'ясування типових проблемних ситуацій. Для підготовки якісних фахівців з інформаційної безпеки ділові ігри повинні охоплювати наступні питання:

- захист від несанкціонованого доступу до інформації. Тобто слід звернути увагу на використання засобів управління доступом користувачів, антивірусне програмне забезпечення (ПЗ), ПЗ для захисту робочих станцій та серверів, спеціалізоване ПЗ для пристроїв вводу-виведення, ПЗ для захисту систем управління базами даних, спеціалізоване ПЗ для попередження витоків інформації (DLP-системи), системи виявлення та попередження вторгнень, системи захисту периметру мережі, proxy-сервери, фільтрація електронної пошти, пристрої для організації криптографічних та захищених з'єднань, системи для збору та обробки подій, сканери уразливості, ПЗ для оцінки захищеності систем та додатків, системи контролю та управління доступом, засоби охорони периметру. Також, слід розглянути засоби, які забезпечують безперервність функціонування бізнесу, а саме: системи резервного копіювання та відновлення, системи забезпечення безперебійного електричного живлення, системи охолодження та клімат-контролю.
- моделювання технічних каналів витоку інформації та каналів спеціального впливу, а також засоби, які використовуються для попередження витоку інформації.

Розглянувши дані засоби, майбутні фахівці матимуть уявлення про технічні пристрої захисту інформації. Однак, цих знань недостатньо для того, щоб стати висококваліфікованим фахівцем. Важливо також вміти управляти системою захисту інформації. Тому в тематику ділових ігор слід включити: процеси організації системи управління інформаційною безпекою, послідовність приведення системи захисту у відповідність до вимог нормативних документів, розрахунок економічної

ефективності заходів захисту, управління ризиками інформаційної безпеки, проведення аудиту інформаційної безпеки.

Другим кроком є підготовка сценарію гри (певної моделі). Сценарій містить порядок дій викладача з моменту повідомлення завдання учасникам і до закінчення гри. Необхідно ретельно, епізод за епізодом, описати очікувані варіанти дій учасників гри з ймовірними мотивуваннями цих дій, поясненнями всіх розрахунків і описом контактів між учасниками.

Третім кроком є розподіл ролей між учасниками гри. Найбільш поширеними ролями для проведення ділових ігор, які сприяють підготовці фахівців з інформаційної безпеки, є реальні посади, які існують у сучасних організаціях: це керівник підприємства (установи, організації), керівник структурного підрозділу, фахівець з організації інформаційної безпеки, менеджер (управитель) систем з інформаційної безпеки, технік з захисту інформації, фахівець із організації захисту інформації з обмеженим доступом, адміністратор безпеки, головний спеціаліст тощо.

Четвертим кроком є визначення правил гри. На даному кроці формується регламент, в якому чітко описано дозволені дії, порядок проведення гри, час проведення гри, інтенсивність гри. У випадку відсутності регламенту може просто не вистачити часу для її завершення і досягнення позитивного результату.

П'ятим кроком є розробка критеріїв та показників оцінювання результатів виконання ігрових дій. Найбільш зручними критеріями оцінки ефективності ділової гри є чіткість та ефективність дій і рішень кожного учасника гри, новизна та обґрунтованість запропонованих заходів, досягнення поставлених цілей.

Шостим кроком є складання інструкції для викладача і студентів; розробка робочих матеріалів для учасників гри. Викладач повинен роз'яснити учасникам ділової гри порядок та особливості її проведення, критерії оцінки результатів, наголосити, що гра має змагальний характер.

Сьомим кроком є проведення ділової гри. Гра починається з оголошення викладачем теми ділової гри, завдання, мети, правил та вручення інструкцій кожному з учасників гри. Після цього викладач повинен надати учасникам час на обдумування її змісту, обговорення ситуації з сумісниками, підлеглими, керівництвом, і лише після цього вимагати відповідних дій і рішень.

Подальші дії викладача полягають в спостереженні, аналізі та фіксуванні всіх дій і рішень кожного із учасників гри, їх взаємодії та корегуванні плану проведення гри.

Восьмим кроком є підведення підсумків і аналіз результатів гри.

Підсумковий аналіз розпочинається з оголошення загальних навчальних цілей. Далі викладач аналізує основні теоретичні (методичні) виробничо-економічні положення, які пов'язані з відповідними рішеннями та діями учасників гри. Після цього у хронологічному порядку розглядаються рішення учасників, розкриваються помилки і показується правильний порядок дій, який виключає допущені помилки [19].

У результаті аналізу основних головних положень у студентів повинно скластися чітке уявлення про те, як їм слід було діяти в конкретних обставинах, створених у діловій грі. Гра закінчується оцінкою дій кожного із учасників.

Для ефективної реалізації методики ділових ігор важливо дотриматися наступних вимог:
- гра повинна бути логічним продовженням і завершенням конкретної теоретичної теми (розділу) навчальної дисципліни, практичним доповненням вивчення дисципліни в цілому;
- максимальна наближеність гри до реальних професійних умов;
- створення атмосфери пошуку й невимушеності;
- ретельна підготовка навчально-методичної документації;
- чітко сформульовані завдання, умови і правила гри;
- виявлення можливих варіантів вирішення зазначеної проблеми;
- наявність необхідного обладнання [20].

На нашу думку ділові ігри слід проводити відразу після проведення лекцій, в яких розкриваються теоретичні аспекти захисту інформації, а на практичних заняттях у формі ділових ігор їх слід закріплювати, розбираючи певні ділові ситуації. Для реалізації практичної складової вищим навчальним закладам необхідно налагодити взаємодію з організаціями, які займаються захистом інформації, а також залучати на час проведення ігор практикуючих співробітників.

Отже, завдяки використанню у навчальному процесі ділової гри, студенти закріплюють здобуті теоретичні знання, глибше пізнають предмет навчання, а також отримують певні практичні навички.

5. ВИСНОВКИ. Метод, описаний в даній статті, дозволить студентам краще осмислити

матеріал, розвинути свої творчі здібності в розв'язанні проблеми захисту інформації, стимулює не тільки розбиратися в тих чи інших питаннях ІБ, але також вчитися працювати в колективі. Вона сприяє створенню цілісної моделі фахівця із захисту інформації та управління інформаційною безпекою, яка, в свою чергу, може бути основою для розвитку цієї сфери професійної діяльності, а також спрямує подальші дослідження форм і методів професійної підготовки фахівців з ІБ.

Ділові ігри допоможуть забезпечити майбутніх фахівців з інформаційної безпеки необхідними теоретичними знаннями та практичними навиками у сфері сучасних методів та засобів захисту інформації. Високий рівень знань в галузі ІБ дозволить підвищити функціональність й надійність інформаційних систем та технологій, що використовуються на об'єктах інформаційної діяльності.

Таким чином, ділова гра є ефективним методом формування професійних навичок і вмінь у студентів і сприяє підвищенню якості підготовки спеціалістів у сфері ІБ.

ЛІТЕРАТУРА

[1]. Указ Про Доктрину інформаційної безпеки України: за станом на 08.07.2009 / Президент України [Електронний ресурс]. – Режим доступу: \www/ URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009

[2]. Постанова Про затвердження Концепції технічного захисту інформації в Україні: за станом на 13.10.2011 / Кабінет Міністрів України [Електронний ресурс]. – Режим доступу: \www/ URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1126-97-%EF

[3]. Постанова Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра: за станом на 01.06.2011 / Кабінет Міністрів України [Електронний ресурс]. – Режим доступу: \www/ URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=787-2010-%EF

[4]. Наказ Про введення в дію переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра / Міністерство освіти і науки України [Електронний ресурс]. – Режим доступу: \www/ URL: http://skviravo.ucoz.ru/Novyny/1067.zip

[5]. Перелік державних вищих навчальних закладів, ліцензованих за напрямами підготовки 1601, 1701 в галузі знань «Інформаційна безпека» [Електронний ресурс]. – Режим доступу: \www/ URL:http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=75762&cat_id=39110&ctime=1231500462175

[6]. Конеев И.Р. Информационная безопасность предприятия. / Конеев И.Р., Беляев А.В. – СПб.:БХВ-Петербург, Проспкт, 2003. – 160 с.

[7]. Проблеми ІТ-освіти в Україні [Електронний ресурс] / Олександр Кардаков. – Режим доступу: \www/ URL: http://osvita.ua/vnz/high_school/17048

[8]. Закон України Про вищу освіту: за станом на 10.02.2010/ Верховна Рада України [Електронний ресурс]. – Режим доступу: \www/ URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2984-14

[9]. Смолкин А.М. Методы активного обучения. – М., 1991. – 207 с., С.30.

[10]. Комплексная деловая игра "Мысль": Методическое пособие/И. Г. Абрамова, М.В. Брагинский. – М., 1991. – 64 с.

[11]. Активные формы и методы обучения, как средство профессионального становления [Електронний ресурс]/Виноградненко Е.А. – Режим доступу: \www/ URL: http://vinogradenko66.rusedu.net/archives/2666/20110207

[12]. Словарь психолога-практика/ [Сост. С.Ю. Головин] – 2-е изд., перераб. и доп. – Мн.: Харвест, 2003. – С.224

[13]. Емельянов С.В. и др. Метод деловых игр. Обзор. / Емельянов С.В., Бурков В.Н., Ивановский А.Г. – М., 1976. – 58 с.

[14]. Гидрович С.Р., Сыроежин И.М. Игровое моделирование экономических процессов (деловые игры). – М.: Экономика, 1976. – 116 с.

[15]. Активное обучение в высшей школе [Електронний ресурс]/Вербицкий А.А. – Режим доступу: \www/ URL: http://www.guma.oglib.ru/bgl/186/336.html

[16]. Казанцев А.К. и др. Практический менеджмент: В деловых играх, хозяйственных ситуациях, задачах и тестах / Казанцев А.К., Подлесных В.И., Серова Л.С. – М.: Академия, 1999. – 365 с.

[17]. Змиевская Е.В. Учебная деловая игра в организации самостоятельной работы студентов педагогических вузов: дис. на соискание уч. степени канд. педагогических наук: спец. 13. 00.01 "общая педагогика, история педагогики и образования" / Змиевская Екатерина Владимировна; московский педагогический государственный университет. - Москва, 2003. - 169 с.

[18]. Самыгин С.И. Педагогика и психология высшей школы. Серия «Учебники, учебные пособия». Ростов-на-Дону: «Феникс», 1998—544с.

[19]. Методика подготовки и проведения деловых игр [Електронний ресурс]. – Режим доступу: \www/ URL:

http://libsib.ru/innovatsionniy-menedzhment/funktsii-innovatsionnogo-menedzhmenta/metodika-podgotovki-i-provedeniya-delovich-igr

[20]. Баранец И.Б. Деловая игра как метод активного обучения [Електронний ресурс]. – Режим доступу: \www/ URL: http://www.rusnauka.com/3_SND_2010/Pedagogica/58102.doc.htm

REFERENCES

[1]. President of Ukraine. (2009) The Decree on Information security doctrine of Ukraine. [Online]. Available from http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009. [Accessed 20/02/13].

[2]. Cabinet of Ministers of Ukraine. (2011) The resolution On Approval Convention of Technical Information Protection in Ukraine. [Online]. Available from http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1126-97-%EF. [Accessed 20/02/13].

[3]. Cabinet of Ministers of Ukraine. (2011) The resolution on approval of list of specialties in which accomplished training the specialists in universities in educational qualification levels of specialist and master. [Online]. Available from http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=787-2010-%EF. [Accessed 20/02/13].

[4]. Ministry of Education and Science of Ukraine. (2011) The order On implementing the list of specialties in which accomplished training the specialists in universities in educational qualification levels of specialist and master. [Online]. Available from http://skviravo.ucoz.ru/Novyny/1067.zip. [Accessed 20/02/13].

[5]. State Service for Special Communication and Information Protection of Ukraine. (n.d.) The list of state universities, licensed in the areas of 1601, 1701 in the field of knowledge "Information Security". [Online]. Available from http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=75762&cat_id=39110&ctime=1231500462175. [Accessed 12/02/13].

[6]. Koneev I.R., Beliaev A.V. (2003) Information security of enterprise. St. Petersburg: Prospect.

[7]. LIGA Business Inform (2011) The problems of IT-education in Ukraine. [Online]. Available from http://osvita.ua/vnz/high_school/17048. [Accessed 10/02/13].

[8]. Verkhovna Rada of Ukraine (2010) Law of Ukraine on higher education. Available from http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2984-14. [Accessed 16/02/13].

[9]. Smolkin A.M. (1991) The method of active learning. Moscow

[10]. Abramova I.G., Braginskii M.V. (1991) The complex business game "Idea": Methodical manual. Moscow

[11]. Vinogradenko E.A. (2011) The active forms and methods of education as a means of professional development. Belgorod.

[12]. Golovin S.Y. (2003) Dictionary of psychologist practice. Minsk: Kharvest.

[13]. Emilianov S.V., Byrkov V.N, Ivanovskii A.G. (1976) The method of business games. Review. Moscow: Economica.

[14]. Gidrovich S.R., Syroezhkin I.M. (1976) Game modeling of economic processes (business game). Moscow

[15]. Verbitskii A.A. (n.d.) Active learning in higher school [Online]. Available from http://www.guma.oglib.ru/bgl/186/336.html. [Accessed 10/02/13].

[16]. Kazancez A.K., Podkolesnykh V.I., Serova L.S. (1999) Practical management: In business games, business situations, tasks and tests. Moscow: Academia.

[17]. Zmievskaia E.V. (2003) The educational business game in the organization independent work of students pedagogical universities. Unpulished thesis (PhD), Moscow pedagogic university.

[18]. Samygin S.I. (1998) Pedagogics and psychology in higher school. Rostov on Don: Fenix.

[19]. Literature for students. (n.d.) The method of preparation and holding business games. [Online]. Available from: http://libsib.ru/innovatsionniy-menedzhment/funktsii-innovatsionnogo-menedzhmenta/metodika-podgotovki-i-provedeniya-delovich-igr. [Accessed 12/02/13].

[20]. Baranets I.B. (n.d.) Business game as a method of active learning. [Online]. Available from: http://www.rusnauka.com/3_SND_2010/Pedagogica/58102.doc.htm. [Accessed 20/02/13].

ДЕЛОВЫЕ ИГРЫ КАК МЕТОД ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение надлежащего уровня информационной безопасности напрямую зависит от качественной профессиональной подготовки будущих специалистов, уровня внедрения и использования инновационных педагогических, информационно-коммуникационных технологий и формирования информационной культуры. Проанализированное современное состояние подготовки специалистов в отрасли информационной безопасности свидетельствует, что текущие требования к умениям и навыкам студентов не соответствуют тем, которые необходимы для построения эффективной системы управления информационной безопасностью организации. В работе раскрыта методика проведения деловых игр для подготовки специалистов в отрасли информационной безопасности. Описанный метод подготовки специалистов позволит студентам лучше осмыслить

материал, развить свои способности в решении проблемы защиты информации, разбираться в тех или иных вопросах информационной безопасности и учиться работать в коллективе. Деловые игры помогут обеспечить будущих специалистов по информационной безопасности необходимыми теоретическими знаниями и практическими навыками в сфере современных методов и средств защиты информации.
Ключевые слова: информационная безопасность; модель высшего профессионального образования; техническая защита; деловые игры; профессиональная подготовка.

BUSINESS GAMES AS A METHOD OF TRAINING INFORMATION SECURITY SPECIALISTS

Providing an adequate level of information security is directly dependent on quality training of future specialists, the level of implementation and use of innovative teaching, infocommunication technologies and information culture. The current state of training specialists of information security industry indicates that the current requirements for skills and experience of students do not consistent with are necessary for building an effective information security management system of the organization. The paper disclosed methodology of business games for training specialists in information security industry. The described method of training will allow students better understand the material, develop their ability in solving the problem of information security, understand some or other questions of information security, and learn to work in teams. The business games help to ensure the future information security professionals necessary theoretical knowledge and practical skills in modern methods and tools of information security.
Index Terms: information security; model of higher education, technical protection, business games, training.

Шиліна Наталія Євгеніївна, кандидат педагогічних наук, доцент, Одеська національна академія зв'язку ім. О.С. Попова.
E-mail: natuccy@mail.ru
Шилина Наталия Евгениевна, кандидат педагогических наук, доцент, Одесская национальная академия связи им. А.С. Попова.
Shylina Nataliia, PhD, associate professor, Odessa National Academy of Telecommunications named after O.S.Popov.

Копитін Юрій Вікторович, комунальне підприємство «Обласний інформаційно-аналітичний центр», т.в.о. начальника відділу забезпечення захисту інформації, Одеська національна академія зв'язку.
E-mail: ykopitin@odessa.gov.ua
Копытин Юрий Викторович, коммунальное предприятие "Областной информационно-аналитический центр", и.о. начальника отдела защиты информации, Одесская национальная академия связи им. А.С. Попова.
Kopytin Yuriy, municipal enterprise "Regional information-analytical center", the acting head of the department of information security, Odessa National Academy of Telecommunications named after O.S.Popov.

УДК 621.391.7

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ ДЛЯ ЗДІЙСНЕННЯ АВТЕНТИФІКАЦІЇ СТОРІН ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрий Яремчук

В роботі розглянуто математичний апарат рекурентних V_k^+ *та* U_k *– послідовностей, а також можливість побудови методу автентифікації сторін взаємодії на його основі. Для запропонованого методу розроблено принципи побудови спеціалізованих процесорів для можливості доведення та перевірки автентичності відповідно кожною із сторін взаємодії. Порівняння швидкості роботи розроблених процесорів з відомими аналогами показало, що за певних умов час роботи розроблених спеціалізованих процесорів автентифікації буде в десятки разів меншим, ніж на процесорах, що реалізують відомі методи. Розроблені спеціалізовані процесори мають перспективи використання в задачах різного криптографічного призначення, що базуються на технології відкритого ключа.*
***Ключові слова**: спеціалізовані процесори, захист інформації, криптографія, автентифікація, рекурентні послідовності.*

Вступ. На сьогодні задача забезпечення цілісності інформації є не менш, а в деяких випадках і більш актуальною, ніж задача конфіденційності інформації. Для забезпечення цілісності розробляються криптографічні протоколи [1-6], найбільш розповсюдженими з яких є два типи протоколів – автентифікації та цифрового підписування. Що стосується автентифікації, то в основ-