

16. Jamaletdinova G.A. Samoupravljenje uczebno-poznavatel'noj dejatel'nost'ju studentov v sfere fizicheskoj kul'tury: monografija / G.A. Jamaletdinova. – Ekaterinburg : Gumanitarnyj universitet, 2008. – 136 s.
17. Diegmann L. Zur Prävention durch Gesundheitserziehung - Beeinflussung von Risikofaktoren im Betriebsgesundheitswesen / L. Diegmann, L. Heinemann, H. Heine, C. Deigmann // Das deutsche Gesundheitswesen. – 1980. - № 33. - S.1305-1309.
18. Hardman A. Physical activity. Healthy lifestyles nutrition and activity. International life sciences institute / A. Hardman. – 1998. - R. 40-46.
19. Piko Bettina Francisco. The roll of physical activity in university students health. XXVII FIMS World Congress of sports medicine. Abstracts book / Bettina Francisco Piko. – Budapest, Hungary, 2002. - 10 p.
20. Szostak W.B. Prewencja chorób sercowo-naczyniowych – postępy 2012 / W.B. Szostak, B. Cybulska, L. Kłosiewicz-Latoszek, D. Szostak // Węgierek Medycyna praktyczna. – 2013. - № 266. - P. 12-22.

### Реферат

МЕДИКО-СОЦІАЛЬНІ АСПЕКТИ НАВЧАЛЬНОЇ АДАПТАЦІЇ У СТУДЕНТІВ МЕДИЧНИХ ВНЗ

Огнев В.А., Кириченко М.П., Зінчук А.М., Огнева Л.Г.

Ключові слова: здоров'я студентів, адаптація, навчальний процес, фактори корекції адаптації, самооцінка здоров'я.

В роботі була зроблена спроба аналізу соціальних та медичних критеріїв адаптації молоді, що навчається, до варіабельних особливостей навчального процесу на протязі ряду років. Особлива увага приділялась двом основним індексам: фізичного здоров'я та ментального здоров'я. Було визначено кілька градацій адаптації. Оцінювалась можливість використання коригуючих факторів для всього організму в цілому та його окремих систем.

### Summary

MEDICAL AND SOCIAL ASPECTS OF EDUCATIONAL ADAPTATION IN MEDICAL STUDENTS

Ognev V.A., Kyrychenko M.P., Zinchuk A.M., Ogneva L.G.

Key words: health students, adaptation, learning process, correction factors adaptation, self-care.

The paper was an attempt to analyze the social and medical criteria to evaluate the adaptation of young people who study at the high schools to teaching process variable features over the years. Particular attention was paid to the two main indices: physical health and mental health. We determined several levels of adaptation and evaluated the possibility to use adjustment factors to the whole organism and its separate systems.

УДК 378.14 : 621.39

**Скрипник І.М., Скрипніков П.М., Гаєвський С.О., Гопко О.Ф., Дубина В.О.**

## ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕМЕДИЧНИХ ТА ТЕЛЕОСВІТНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

ВДНЗУ «Українська медична стоматологічна академія», м. Полтава

*Проаналізовано кількість атак та їх типи на освітньому порталі факультету післядипломної освіти Української медичної стоматологічної академії. Виявлено навмисні інформаційні загрози, створені зловмисниками з метою отримання несанкціонованого доступу до сервера.*

Ключові слова: телемедицина, дистанційна освіта, захист інформації

Сьогодні в Україні у зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Створюються локальні і регіональні обчислювальні мережі, великі території охоплені мережами сотового зв'язку, факсиміальний зв'язок став доступний для широкого кола користувачів. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери.

На фоні швидкого впровадження інформаційних технологій неминуче виникають проблеми, пов'язані з захистом персональних та корпоративних даних від ненавмисного та навмисного втручання в роботу інформаційних систем.

Проблема інформаційного захисту не є чисто технічною, значною мірою вона визначається також соціальними та

адміністративними чинниками, а саме кваліфікацією персоналу та внутрішніми правилами безпеки у закладі.

Динамічні зміни в економіці, науці та суспільстві, розвиток інноваційних технологій спонукають зміни і в сфері медицини та післядипломної медичної та фармацевтичної освіти, а саме розробки, наукового обґрунтування та практичної апробації загальних рекомендацій та конкретних шляхів забезпечення комплексного захисту персональних та корпоративних даних в сучасних телемедичних та телеосвітніх системах.

На фоні тотальної глобалізації обміну інформацією виникають проблеми контролю її розповсюдження, обмеження доступу до конфіденційних даних, запобігання несанкціонованого втручання в роботу комп'ютерних систем. В останній час почастишали інциденти, пов'язані з порушення інформаційної безпеки, що призвели до витоку,

спотворення або втрати конфіденційних даних, внаслідок чого виникали значні матеріальні та моральні збитки.

Метою дослідження стало підвищення інформаційної безпеки в галузі дистанційної медичної післядипломної освіти, а саме запобігання витоку конфіденційної інформації та несанкціонованого втручання в роботу комп'ютерних систем.

Проведений аналіз інформаційних загроз на тренінговому порталі факультету післядипломної освіти ВДНЗУ «Українська медична стоматологічна академія», що був створений для більш ефективного тренінгу розроблений та впроваджений в обов'язкову підготовку до іспитів «Крок-3 Загальна лікарська підготовка» та «Крок-3 Стоматологія», та дає змогу лікарям-інтернам тренуватися в зручний для них позааудиторний час. Портал доступний за інтернет-адресами

відповідно <http://medtest.dentaero.com/> та <http://test.dentaero.com/>

Користуватися порталом можливо за допомогою будь-якого стаціонарного чи мобільного пристрою (стаціонарні комп'ютери, ноутбуки, планшети, мобільні телефони) з дротовим чи бездротовим способом під'єданого до мережі Інтернет. Забезпечується індивідуальний захищений доступ користувачів з використанням попередньої реєстрації та особистого паролю. Окремий тест включає 200 тестових завдань, випадково вибраних з бази понад 2000 тестів іспитів за десять попередніх років. В сформований варіант тесту переважно включаються ті завдання, на які конкретний користувач дав помилкову відповідь під час попередніх тестувань. Таким чином забезпечується індивідуалізація тренінгу з повторенням більш складних для користувача тем. Надана можливість в будь-який момент перервати тестування та отримати проміжний результат.

Загальні результати тестування окремо по кожному користувачеві, час його активного перебування на порталі, кількість опрацьованих тестів доступні для аналізу адміністратором порталу (деканатом післядипломної освіти) та можуть бути представлені у вигляді рейтингу як рівня підготовки користувачів, так і ступеня засвоєння тематичних розділів, що опановуються на відповідних кафедрах. Таким чином, реалізовано механізм ефективного виявлення потенційно відстаючих лікарів-інтернів, що потребують індивідуальних занять, а також визначення розділів, більш складних для опанування, з подальшим можливим перерозподілом навчального часу та покращенням їх методичного забезпечення.

Пілотне впровадження обов'язкового тренінгу з використанням інтернет-порталу в 2013 році для лікарів-інтернів, які безпосередньо перед іспитом навчалися на заочних базах стажування, показало високу ефективність як са-

ме тренінгу, так і отриманих важелів для індивідуальної роботи з лікарями-інтернами. Виявлялася виражена кореляція між загальною кількістю опрацьованих на порталі питань та індивідуальним результатом наступного іспиту.

З метою забезпечення цілісності та конфіденційності інформації було досліджено рівень інформаційної безпеки порталу, частоту навмисних та ненавмисних порушень під час активної роботи користувачів та детально проаналізовано реальні випадки інформаційних загроз відповідно до вищенаведених класифікацій.

Основна інформація порталу, що підлягала захисту, включала базу тестових питань та архів результатів тестування. Хоча база питань була відкрита (використовувалися питання іспитів «Крок-3» минулих років, що знаходилися в публічному доступі, зокрема, на веб-сторінці Центру тестування при МОЗ України), особливості функціонування тестового порталу визначали необхідність часткового інформаційного захисту, а саме тимчасових варіантів тестових завдань, сформованих для кожного лікаря-інтерна індивідуально. Логіка навчального процесу передбачала цільове формування тестового варіанту передбачала урахування попередніх результатів та помилок конкретного користувача з метою найбільш ефективного засвоєння матеріалу саме тих розділів, які були проблемними для конкретного лікаря-інтерна. Також для зручності роботи з порталом передбачалася можливість тимчасової паузи в тестуванні зі збереженням як результатів, так і сформованого тестового варіанту. Таким чином, виникала ймовірність попереднього ознайомлення із запропонованим тестовим варіантом шляхом організації витоку інформації з використанням несанкціонованого доступу до бази даних тимчасових варіантів на сервері.

Інша потенційна загроза передбачала активний доступ злоумисника до архіву тестування з метою спотворення інформації про результати тестування конкретних користувачів або взагалі знищення архіву в цілому з метою приховування негативних результатів окремого користувача.

Також існувала можливість проведення мережевих атак відмови в обслуговуванні (DDoS) з метою правдоподібного пояснення низької активності конкретного користувача у порівнянні з іншими.

Для виявлення випадків і способів проведення інформаційних атак та оцінки її активності та успішності проводився аналіз логів хостинг-провайдера та власне порталу з використанням PHP-скриптів, спеціально розроблених для виявлення та оцінки наслідків подібних атак, а також оперативного цілодобового (24/7) інформування адміністратора для оперативного аналізу та запобігання в «ручному» режимі.

Протягом року активного функціонування порталу (01.01.2014 – 01.01.2015) зафіксовано 318 інформаційних інцидентів, з них: DDoS – 225 (70,7%), атаки на отримання несанкціонованого доступу до ресурсу хостинг-провайдера – 52 (16,4%), атаки типу “крадіжка особистості” (включаючи спроби підбору індивідуальних паролів доступу до особистих сто-

рінок користувачів ресурсу) – 27 (8,5%), спроби отримання адміністративного доступу до ресурсу (підбір паролів адміністраторів та аудиторів) – 12 (3,8%), SQL-ін'єкції з метою отримання доступу до баз даних ресурсу – 2 (0,6%). Розподіл атак за типами представлений на рис 1.

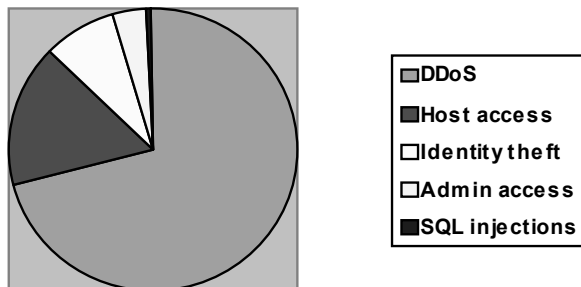


Рис. 1. Розподіл за типами інформаційних атак на навчально-контролюючий інтернет-портал факультету післядипломної освіти ВДНЗУ “УМСА” за період 01.01.2014 – 01.01.2015 року.

Найбільша активність зловмисників спостерігалась в осінньо-зимовий період, що відповідало загальному сезонному розподілу загальної мережевої активності користувачів. Відмічений короткочасний зріст активності у березні (18,2% всіх атак на протязі календарного року) відповідав підвищенню активності користувачів

порталу у період активної підготовки до іспиту “Крок-3”, що вказує на зв'язок виявлених інформаційних інцидентів з безпосереднім функціонуванням порталу та може свідчити про наявність інформаційних загроз у цей період (рис 2).

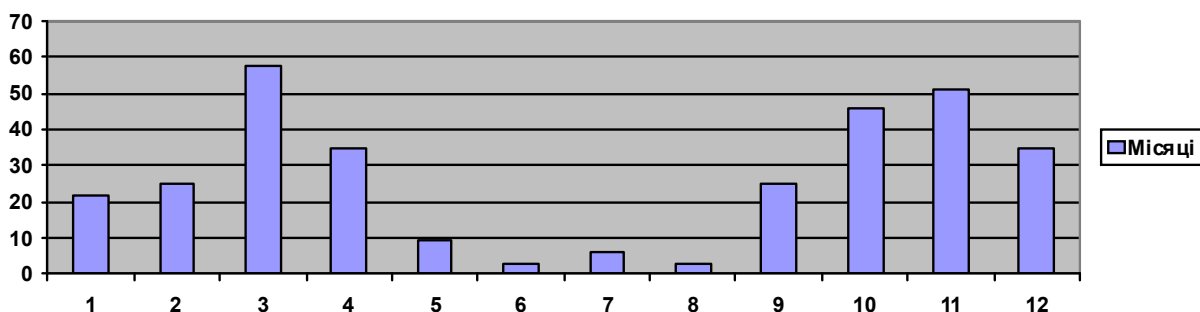


Рис.2. Сезонний розподіл активності інформаційних атак на навчально-контролюючий інтернет-портал факультету післядипломної освіти ВДНЗУ “УМСА” за період 01.01.2014 – 01.01.2015 року.

Таким чином, серед інцидентів, пов'язаних з інформаційною безпекою, переважали неспецифічні мережеві DDoS-атаки. Випадки специфічних атак, що можуть бути класифіковані як навмисні, включав атаки типу “крадіжка особистості”, спрямовані на отримання несанкціонованого адміністративного доступу до ресурсу або несанкціонованого доступу до особистої сторінки учасника. Активність таких атак була значно вищою безпосередньо у період активного тренінгу перед іспитом “Крок-3”.

### Література

1. Берко А.Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / А.Ю. Берко, В.А. Висоцька, І.В. Рішняк // Вісник Національного університету “Львівська політехніка”. - 2008. - № 610. - С. 20-33.
2. Гуцу С.Ф. Правові основи інформаційної діяльності [Електронний ресурс]. - Режим доступу : <http://studrada.com.ua>

3. Золотар О.О. Класифікація загроз інформаційної безпеки / О.О. Золотар, І.О. Трубін // Інформація і право - 2013. - №3(9) - С. 105-112.
4. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук. : спец. 12.00.01 “Теорія та історія держави і права; історія політичних і правових вчень” / Ю.Є. Максименко. - К., 2007. - 22 с.
5. Марущак А.І. Пріоритети розвитку інформаційного права України / А.І. Марущак // Інформація і право. - 2011. - № 1. - С. 20-24.
6. Олійник О.В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 “Адміністративне право і процес; фінансове право; інформаційне право” / О.В. Олійник. - К., 2006. - 20 с.
7. Пилипчук В.Г. Системні проблеми розвитку правової науки в інформаційній сфері / В.Г. Пилипчук // Вісник Академії правових наук України. - 2011. - № 3. - С. 16-27.
8. Погребняк А.В. Технології комп'ютерної безпеки : [монографія] / Погребняк А. В. - Рівне : МЕРУ, 2011. - 117 с.

### References

1. Berko A.Yu. Metody ta zasoby otsinyuvannya ryzykiv bezpeky informatsiyi v systemakh elektronnoyi komertsiyi / A.Yu. Berko, V.A. Vysots'ka, I.V. Rishnyak // Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika". - 2008. - № 610. - S. 20-33.
2. Hutsu S.F. Pravovi osnovy informatsiyoi diyal'nosti [Elektronnyy resurs]. - Rezhym dostupu : <http://studrada.com.ua>
3. Zolotar O.O. Klasyfikatsiya zahroz informatsiyoi bezpeky / O.O. Zolotar, I.O. Trubin // Informatsiya i pravo - 2013. - №3(9) - S. 105-112.
4. Maksymenko Yu.Ye. Teoretyko-pravovi zasady zabezpechennya informatsiyoi bezpeky Ukrainy : avtoref. dys. na zdobuttya nauk. stupenya kand. yuryd. nauk. : spets. 12.00.01 "Teoriya ta istoriya derzhavy i prava; istoriya politychnykh i pravovykh vchen'" / Yu.Ye. Maksymenko. - K., 2007. - 22 s.
5. Marushchak A.I. Priorytety rozvytku informatsiyoho prava Ukrainy / A.I. Marushchak // Informatsiya i pravo. - 2011. - № 1. - S. 20-24.
6. Oliynyk O.V. Orhanizatsiyno-pravovi zasady zakhystu informatsiynykh resursiv Ukrainy : avtoref. dys. na zdobuttya nauk. stupenya kand. yuryd. nauk. : spets. 12.00.07 "Administratyvne pravo i protses; finansove pravo; informatsiyne pravo" / O.V. Oliynyk. - K., 2006. - 20 s.
7. Pylypchuk V.H. Systemni problemy rozvytku pravovoyi nauky v informatsiyoi sferi / V.H. Pylypchuk // Visnyk Akademiyi pravovykh nauk Ukrainy. - 2011. - № 3. - S. 16-27.
8. Pohrebnyak A.V. Tekhnolohiyi komp'yuternoyi bezpeky : [monohrafiya] / Pohrebnyak A. V. - Rivne : MEHU, 2011. - 117 s.

### Реферат

#### ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕМЕДИЦИНСКИХ И ТЕЛЕОБРАЗОВАТЕЛЬНЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

Скряпник И.Н., Скрипников П.Н., Гаевский С.А., Гопко А.Ф., Дубина В.А.

Ключевые слова: телемедицина, дистанционное образование, защита информации

Проанализированы количество атак и их типы на образовательном портале факультета последипломного образования Украинской медицинской стоматологической академии. Выявлено умышленные информационные угрозы, созданные злоумышленниками с целью получения несанкционированного доступа к серверу.

### Summary

#### INFORMATION SECURITY OF TELEMEDICINE AND TELELEARNING COMPUTER SYSTEMS

Skrypnik I.N., Skrypnikov P.N., Hayevskiy S.A., Hopyko A. F., Dubina B.A.

Key words: telemedicine, distance education, information, telelearning, information security

This research paper presents in-depth study of the number and the types of attacks registered at the educational portal of the Faculty of Postgraduate Education, Ukrainian Medical Stomatological Academy. There have been revealed deliberate information threats designed by intruders to gain unauthorized access to the server.

УДК 611-018:378.661

**Сулаева О.Н.**

### ОТБОР СОДЕРЖАНИЯ ОБУЧЕНИЯ ПО ГИСТОЛОГИИ В ДОСТИЖЕНИИ СТАНДАРТОВ МЕДИЦИНСКОГО ОБРАЗОВАНИЯ

Запорожский государственный медицинский университет

*Важнейшим фактором повышения эффективности обучения в медицинском вузе является разработка системы достижения стандартов качества обучения. Последнее особенно важно при изучении фундаментальных медицинских дисциплин, включая гистологию, поскольку конечной целью изучения гистологии в медицинском вузе является не подготовка гистолога или выяснение подробностей структурной организации органов и тканей, а формирование фундаментальных знаний, облегчающих понимание принципов функционирования и регуляции организма человека в норме и при патологии. В этом контексте предложена концепция отбора содержания обучения гистологии, основанная на клинической мотивации и междисциплинарной интеграции, позволяющая реализовать сквозную программу обучения и повысить коэффициент полезного действия при изучении фундаментальных медицинских наук.*

Ключевые слова: качество обучения, гистология, сквозная программа обучения.

Современная стратегия развития высшего медицинского образования ориентирована на подготовку компетентных специалистов, основные квалификационные характеристики которых базируются на системе стандартов высшего образования [4]. Однако скачок научно-технического прогресса внес свои коррективы в эту стратегию, поскольку развитие новых технологий и внедрение новых методов диагностики и терапии в практическую медицину стало опережать темпы обновления образовательных ресурсов [3]. Ярким подтверждением этого положения могут быть результаты исследований в области молекулярной биологии

и генетики, клеточной и геномной терапии, нанотехнологии и др. Увы, но современная высшая медицинская школа оказалась не готовой не только предвидеть этот научный прорыв, но и адаптировать систему обучения под существующие реалии [5]. Как результат, центр подготовки молодых специалистов переместился из ВУЗов в ведущие медицинские центры, обладающие необходимыми ресурсами. И, к сожалению, сегодня в успешных частных клиниках знают основы репаративной медицины и клеточных технологий гораздо лучше, чем это отражено в учебной литературе и программах подготовки врачей. Порочный круг замкнулся.