ТИРАСПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи
C.Z.U.: 378.091:004.056(043.3)

БОГДАНОВА ВИОЛЕТТА

МЕТОДИКА ИЗУЧЕНИЯ В ВЫСШЕМ ОБРАЗОВАНИИ ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

532.02 – ШКОЛЬНАЯ ДИДАКТИКА
(ПО СТУПЕНЯМ ОБУЧЕНИЯ И ДИСЦИПЛИНАМ)

Диссертация доктора педагогических наук

Научный руководитель: Кирияк Любомир
Доктор хабилитат,
профессор университета

Автор:

КИШИНЭУ 2022

UNIVERSITATEA DE STAT DIN TIRASPOL

Cu titlul de manuscris
C.Z.U.: 378.091:004.056(043.3)

BOGDANOVA VIOLETA

METODOLOGIA STUDIERII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR A TEHNOLOGIILOR DE PROTECȚIE ȘI SECURITATE A INFORMAȚIEI

532.02 – DIDACTICĂ ŞCOLARĂ
(PE TREPTE ŞI DISCIPLINE DE ÎNVĂŢĂMÂNT)

Teză de doctor în științe ale educației

Conducător ştiinţific: Chiriac Liubomir,
doctor habilitat, profesor universitar

Autorul:

CHIŞINĂU 2022

ОГЛАВЛЕНИЕ

АННОТАЦИЯ

БОГДАНОВА Виолетта

«Методика изучения в высшем образовании технологий защиты информации и информационной безопасности»,

диссертация доктора педагогических наук, Кишинэу, 2022.

Структура диссертации: введение, три главы, общие выводы и рекомендации, библиографический список из 189 наименований, 16 приложений, 131 страница базового текста, 24 рисунка, 23 таблицы. По материалам диссертационного исследования опубликовано 33 печатные работы.

Ключевые слова: информационная безопасность, педагогическая модель, балльно-рейтинговая система оценивания, образовательный веб-квест, самостоятельная работа, интернет технологии, педагогический эксперимент, кибернетический подход, системный подход.

Цель исследования – состоит в теоретическом обосновании, разработке и проверке экспериментальным путем педагогической модели обучения будущих специалистов финансово-экономической сферы технологиям защиты информации и информационной безопасности посредством интернет-технологий.

Задачи исследования: (1) сформулировать методические принципы и подходы, необходимые для проектирования дидактической системы обучения будущих специалистов финансово-экономической сферы дисциплине «Информационная безопасность»; (2) концептуализировать показатели оценивания, критерии и дескрипторы достижений для обеспечения эффективности учебного процесса при изучении информационной безопасности; (3) разработать педагогическую модель обучения будущих специалистов финансово-экономической сферы дисциплине «Информационная безопасность», отражающую содержательную часть дисциплины и методическую систему формирования компетенций в области информационной безопасности; (4) разработать учебно-методический комплекс дисциплины «Информационная безопасность» с использованием информационных технологий, в том числе интернет-технологий; (5) разработать, внедрить и экспериментально проверить эффективность спроектированной педагогической модели и оптимизировать учебный процесс посредством использования новых информационных технологий.

Научная новизна и оригинальность исследования состоит в концептуальном обосновании педагогической модели проектирования и реализации вузовской дисциплины «Информационная безопасность» посредством внедрения интернет-технологий.

Решенная научная задача заключается в определении теоретико-методологических основ обеспечения эффективности изучения вузовской дисциплины «Информационная безопасность», что привело к теоретическому обоснованию и разработке педагогической модели преподавания-обучения-оценивания университетского курса посредством интернет-технологий, ориентированных на процесс формирования профессиональных компетенций будущих специалистов финансово-экономической сферы.

Теоретическая значимость исследования заключается в исследовании и оценивании применения интернет-технологий в процессе формирования и развития профессиональных компетенций в области информационной безопасности у будущих специалистов финансово-экономической сферы с точки зрения разработанной педагогической модели.

Практическая значимость исследования определяется эффективной реализацией разработанной педагогической модели и использованием разработанной методологии обучения в процессе обучения вузовской дисциплине «Информационная безопасность» студентами финансово-экономической сферы посредством применения интернет-технологий, с целью формирования и развития профессиональных компетенций в области защиты информации и информационной безопасности.

Внедрение результатов исследования было осуществлено в образовательный процесс Тираспольского Государственного Университета (г. Кишинэу), Бендерского политехнического филиала Университета им. Т. Г. Шевченко, Тираспольского филиала Московской академии экономики и права, Тираспольского филиала «РОСНОУ»

ADNOTARE

Bogdanova Violeta

"*Metodologia studierii în învățământul superior a tehnologiilor de protecție și securitate a informației*",

Teză de doctor în ştiinţe ale educației, Chişinău, 2022.

Structura tezei: introducere, trei capitole, concluzii generale și recomandări, bibliografie din 189 surse, 16 anexe, 131 pagini text de bază, 24 figuri, 23 tabele. Publicații pe temele tezei 33 de lucrări științifice.

Cuvinte cheie: securitatea informației, model pedagogic, sistem de notare, web quest educațional, lucrul independent, internet tehnologii, experiment pedagogic, abordare cibernetică, abordare sistemică.

Scopul cercetării: constă în fundamentarea teoretică, elaborarea şi validarea pe cale experimentală a modelului pedagogic de studiere a tehnologiilor de protecție și securitate informațională de către viitorii specialişti din domeniul economico-financiar, prin intermediul tehnologiilor internet.

Obiectivele cercetării: 1) formularea principiilor și abordărilor metodologice necesare pentru proiectarea unui sistem didactic de formare a viitorilor specialiști din domeniul economico-financiar la disciplina „Securitatea informațională"; 2) conceptualizarea indicatorilor de evaluare, a criteriilor şi a descriptorilor de performanţă privind studierea securității informaționale pentru asigurarea eficienței procesului instructiv; 3) elaborarea unui model pedagogic de studierea a disciplinei „Securitatea informațională" de către viitorii specialiști din domeniul economico-financiar care reflectă conținutul disciplinei și sistemul metodologic de formare a competențelor în domeniul securității informaționale; 4) dezvoltarea unui complex educațional și metodologic al disciplinei „Securitatea informațională" folosind tehnologii informaționale, inclusiv tehnologiilor internet; 5) elaborarea, implementarea și validarea experimentală a eficienței modelului pedagogic elaborat și optimizarea procesului instructiv prin valorificarea noilor tehnologii informaționale.

Noutatea și originalitatea ştiinţifică rezultatelor cercetării constă în fundamentarea conceptuală a modelului pedagogic de proiectare și realizare a cursului universitar "Securitate Informațională" prin implementarea tehnologiilor internet.

Problema științifică rezolvată rezidă în determinarea fundamentelor teoretice și metodologice ale eficientizării procesului de studiere a disciplinei universitare „Securitatea Informațională", fapt ce a condus la fundamentarea teoretică și elaborarea modelului pedagogic de predare-învățare-evaluare a cursului universitar prin intermediul tehnologiilor internet, orientat spre procesul de formare a competențelor profesionale ale viitorilor specialiști din domeniul economico-financiar.

Semnificația teoretică a lucrării constă în cercetarea și valorificarea tehnologiilor internet în procesul de formare și dezvoltare a competențelor profesionale privind securitatea informațională la studenții din domeniul economico-financiar din perspectiva modelului pedagogic elaborat.

Valoarea aplicativă a lucrării este determinată de implementarea eficientă a modelului pedagogic elaborat și utilizarea metodologiei de instruire dezvoltate în procesul de studiu al cursului universitar "Securitatea informațională", pentru studenții din domeniul economico-financiar, prin aplicarea tehnologiilor internet, în scopul formării și dezvoltării competențelor profesionale privind protecția și securitatea informațională.

Implementarea rezultatelor cercetării a fost realizat în procesul educațional al Universității de Stat din Tiraspol (or. Chișinău), Filiala Politehnică din Bender a Universității "T. G. Shevchenko", filiala din Tiraspol a Academiei de Economie și Drept din Moscova, filiala din Tiraspol a "ROSNOU".

ANNOTATION

Bogdanova Violeta

"Methodology for studying information protection and security technologies in higher education",

dissertation of Doctor of Educational Sciences, Chisinau, 2022

Thesis structure: introduction, three chapters, general conclusions and recommendations, bibliography from 189 sources, 16 annexes, 131 pages of base text, 24 figures, 23 tables. Publications on the topics of the thesis 33 scientific works.

Keywords: information security, pedagogical model, scoring system, educational web quest, independent work, Internet technologies, pedagogical experiment, cybernetic approach, systemic approach.

Aim of the research: consists in the theoretical substantiation, elaboration and experimental validation of the pedagogical model for the study of information protection and security technologies by the future specialists in the economic-financial domain, via internet technologies.

Objectives of the research: 1) the formulation of the principles and methodological approaches necessary for the design of a didactic system for the training of future specialists in the economic-financial domain in the discipline "Information security"; 2) conceptualization of evaluation indicators, criteria and performance descriptors regarding the study of information security to ensure the efficiency of the instructional process; 3) the elaboration of a pedagogical model for the study of the discipline “Information security” by the future specialists in the economic-financial domain that reflects the content of the discipline and the methodological system of skills training in the field of information security; 4) development of an educational and methodological complex of the discipline "Information security" using information technologies, including Internet technologies; 5) elaboration, implementation and experimental validation of the efficiency of the developed pedagogical model and optimization of the instructional process by recovering on new information technologies.

The scientific novelty and originality of the research results consists in the conceptual substantiation of the pedagogical model of design and implementation of the university course "Information Security" by implementing internet technologies.

The solved scientific problem consist in determining the theoretical and methodological foundations of the efficiency of the study process of the university discipline "Information Security", which led to the theoretical substantiation and elaboration of the pedagogical model of teaching-learning-evaluation of the university course through internet technologies, the process of training the professional skills of future specialists in the economic-financial domain.

The theoretical significance of the paper: consist in the research and evaluation of internet technologies in the process of formation and development of professional skills on information security for students in the economic-financial domain from the perspective of the pedagogical model developed.

The practical significance of the research: is determined by the efficient implementation of the developed pedagogical model and the use of the training methodology developed in the study process of the university course "Information Security", for students in the economic-financial domain, by applying Internet technologies to train and develop professional skills on information protection and security.

Implementation of the research results was carried out in the educational process of the State University of Tiraspol (Chisinau), Bender Polytechnic Branch of the University T. G. Shevchenko, Tiraspol branch of the Moscow Academy of Economics and Law, Tiraspol branch of "ROSNOU"

ЛИСТ АББРЕВИАТУР

ВО – высшее образование

ВСНП – Всекитайское собрание народных представителей

ГОУ – государственное образовательное учреждение

ЕРК – Европейская рамка квалификаций

ЗУН – знания, умения, навыки

ИКТ – информационно-коммуникационные технологии

ИТ – информационные технологии

КГ – контрольная группа

НИОКР – научно-исследовательские и конструкторские разработки

НОУ– некоммерческое образовательное учреждение

НРК – Национальная рамка квалификаций

ООП – основная образовательная программа

ОПК – Общепрофессиональная компетенция

ОС – операционная система

ООН – Организацияя Объединенных Наций

ПК – профессиональная компетенция

РМ – Республика Молдова

РФ – Российская Федерация

РОЦИТ – Региональный общественный центр интернет технологий

ТФ – Тираспольский филиал

ФГОС – Федеральный государственный образовательный стандарт

ЭГ – эксперментальная группа

ЮНЕСКО – специализированное учреждение Организации Объединённых Наций по вопросам образования, науки и культуры

ENISA – Агентство Европейского Союза по сетевой и информационной безопасности (European Union Agency for Cybersecurity)

GDPR – Общий регламент по защите данных ЕС (General Data Protection Regulation)

ВВЕДЕНИЕ

Актуальность и важность темы. Современные стремительно происходящие изменения в обществе и экономике, бурное развитие науки и техники, предъявляют высокие требования к цифровым компетенциям специалистов различного профиля. Одна из старейших европейских исследовательских и консалтинговых компаний *Ecorys* предлагает правительствам сфокусировать политику образования на навыках, имеющих стратегическое значение для нации, а именно: цифровой грамотности. К базовым навыкам цифровой грамотности отнесены навыки использования цифровых приложений для общения и выполнения базового поиска в Интернете, а также информационная безопасность[1]. *Конфедерацией Британской Промышленности (CBI)* ставится амбициозная цель обучения цифровой грамотности на базовом уровне 100% сотрудников в Великобритании к 2025 году для расширения прав и возможностей людей, развития экономики[2]. *Институт ЮНЕСКО по информационным технологиям и образованию* также называет информационную безопасность одной из составляющих цифровой грамотности[3]. Такой подход находит отклик в *европейской рамке квалификаций для образования и обучения на всем протяжении жизни* (EPK).

Нарушение информационной безопасности на современном этапе развития общества происходит в сфере государственного управления, коммерческой и общественной деятельности, затрагивает права личности. Высокий уровень кибербезопасности защищает от злонамеренных действий в киберпространстве, которые угрожают экономике и образу жизни каждого гражданина[4]. Влияние информационных технологий на социальные и экономические отношения продолжает увеличиваться, информация становится ценным ресурсом, соответственно умение ее защищать ставит новые задачи в подготовке будущих специалистов, в том числе экономических кадров.

В Республике Молдова, как и во всем мире, происходит цифровая трансформация экономики. Законодательство Республики Молдова гармонизируют с законодательством

---

[1] Отчет Ecorys «Digital skills for the UK economy 2016» [online]. *Информационный веб-сайт государственного сектора Соединенного Королевства*, 2016 [citat 23.10.2021]. Доступен: www.gov.uk/government/publications/digital-skills-for-the-uk-economy

[2] Отчет «Обеспечение навыков для новой экономики» [online]. *Сайт Конфедерации британской промышленности (CBI),* 2019 [citat 23.10.2021]. Доступен: www.cbi.org.uk/articles/delivering-skills-for-the-new-economy/

[3] *Институт ЮНЕСКО по информационным технологиям в образовании*. ИИТО ЮНЕСКО © 1997-2022 [citat 23.10.2021]. Доступен: https://iite.unesco.org/ru/

[4] Кибербезопасность в программе DIGITAL Europe [online]. *Цифровая Европейская Программа,* 2021 [citat 23.10.2021]. Доступен: https://digital-strategy.ec.europa.eu/en/activities/cybersecurity-digital-programme

Европейского Союза в рамках Соглашения об ассоциации от 27 июня 2014 года. На основании Концепции информационной безопасности Республики Молдова от 21 декабря 2017 года[5], Парламентом Постановлением №257 от 22.11.2018 утверждена Стратегия информационной безопасности Республики Молдова на 2019–2024 годы и План действий по ее реализации[6].

В Законе Республики Молдова об утверждении Концепции информационной безопасности Республики Молдова № 299 от 21 декабря 2017 года сформулированы задачи обеспечения защиты основных прав и свобод, демократии и правового государства в информационном пространстве в Республики Молдова, в том числе:

1) «*развитие системы подготовки кадров в области информационной безопасности*»;

2) «*развитие культуры информационной безопасности*».

Пути решения этих задач представлены в Постановлении Парламента Республики Молдова об утверждении Стратегии информационной безопасности Республики Молдова на 2019–2024 годы и Плана действий по ее реализации (Приложение 1).

Компетенции в области информационной безопасности названа частью цифровой компетентности международной экономической организацией развитых стран OECD (Organisation for Economic Cooperation and Development) в отчете «*Skills for a Digital World 2016*», наряду с информационной, коммуникационной, умением создавать контент, решать проблемы. В отчете в разделе «цифровая безопасность» выделены составляющие: личная защита, защита данных, защита цифровой личности, меры безопасности, безопасное и стабильное использование [7, с.27].

В ряде европейских стран, а также стран англосферы (Великобритания, США, Канада, Австралия, Ирландия и Новая Зеландия) наблюдается тенденция развития компетенций в области кибербезопасности для снижения рисков и повышения экономического потенциала. Чтобы занять лидирующие позиции в данной области, такие страны как США, Франция, Финляндия, Израиль, Эстония, Нидерланды приняли решение развивать свою индустрию кибербезопасности, инвестируя в образование, исследования и

---

[5] Закон Республики Молдова об утверждении Концепции информационной безопасности Республики Молдова: № 299 от 21 декабря 2017 года. В: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.

[6] Постановление Парламента Республики Молдова об утверждении Стратегии информационной безопасности Республики Молдова на 2019–2024 годы и Плана действий по ее реализации: №257 от 22.11.2018. В: *Monitorul Oficial al Republicii Moldova*, 2019, nr. 13-21, 80.

[7] Отчет OECD «Skills for a Digital World 2016» [online]. *Сайт Международного союза электросвязи (ITU)*, 2016 [citat 23.10.2021]. Доступен: https://www.itu.int/en/ITU-D/Digital-Inclusion/Women-and-Girls/Girls-in-ICT-Portal/Documents/OECD%20skills%20for%20a%20digital%20world.pdf

разработки в определенных регионах, создавая инновационные центры и кластеры предпринимательских проектов. Во всех случаях ключевым компонентом является сотрудничество правительства, академических кругов и частного сектора.

В Европейском Союзе эстонский опыт образования в области информационных технологий и кибербезопасности, развиваемый при поддержке НАТО, имеет хорошую репутацию. Таллиннский технологический университет (TalTech) готовит специалистов в области информационной безопасности. Бакалаврам по направлению подготовки «Прикладная экономика» («Applied Economics») в рамках дисциплины «Обработка данных» изучается тема «Защита данных» («Data protection»)[8].

В Румынии в Университете Бабеша-Бойяи Факультет экономики и управления бизнесом, активно взаимодействуя с бизнес и академической средой, государственными, правоохранительными органами, работают в рамках проекта с 2021 года по теме «Интеллектуальный анализ и прогнозирование экономических и финансовых преступлений в кибервзаимосвязанной деловой среде (FINCRIME)».[9]

В Университете “Alexandru Ioan Cuza” din Iaşi (Румыния) на Факультете экономики и делового администрирования для 2021 года набора по специальности лицензиат «Экономическая информатика» в учебном плане на третьем курсе запланирована дисциплина «Безопасность информационных систем, на втором курсе специальности «Бухгалтерские и управленческие информационные системы» – дисциплина «Защита и безопасность информационных систем» [10].

В области киберзащиты крупнейшим в мире партнерством академических кругов, правительства и частного сектора является инновационный парк Cyberspark в израильском Беэр-Шева. За счет инвестиций и продвижения своих продуктов в крупнейшем израильском вузе – Университете Бен-Гуриона – реализуется множество образовательных программ и НИОКР в области информационной безопасности. В США, крупнейшем в мире поставщике продуктов кибербезопасности, есть исследовательские центры в Кремниевой долине и на Восточном побережье. Во всех случаях цель таких региональных кластеров состоит в использовании образования и исследований в области

---

[8] *Школа информационных технологий: Учебные планы*. TalTech, ©2022 [citat 04.01.2022]. Доступен: https://taltech.ee/en/bachelors-studies-it

[9] Семинар «Интеллектуальный анализ и прогнозирование экономической и финансовой преступности в кибернетической взаимосвязи деловой среды (fincrime)» [online]. *Сайт Университета Бабеша-Бойяи (UBB),* 2022 [citat 04.01.2021]. Доступен: https://news.ubbcluj.ro/event/workshopul-analiza-inteligenta-si-predictia-criminalitatii-economice-si-financiare-intr-un-mediu-de-afaceri-interconectat-cibernetic-fincrime-desfasurat-la-ubb/

[10] *Факультет экономики и делового администрирования: Учебные планы*. Universitatea Alexandru Ioan Cuza din Iași, ©2022 [citat 04.01.2022]. Доступен: https://www.feaa.uaic.ro/programe-de-licenta/planuri-de-invatamant/

кибербезопасности как в интересах национальной безопасности, так и с целью извлечения экономических выгод.

По данным портала bachelorstudies.com, предоставляющем информацию о программах бакалавриата по всему миру, в 2022 году подготовку и переподготовку в области кибербезопасности предлагают 62 высших учебных заведений США, 10 – Великобритании, 2 – Германии [11].

В США в 1989 году создан Технологический институт SANS, который занимается только обучением в области кибербезопасности. Институт организует курсы послевузовского образования, а также готовит по программам бакалавриата и магистратуры в области информационной безопасности [12].

Курсы по информационной безопасности серьезно изучают во всех странах, где на национальном уровне принимают документы по политике безопасности в области информационных технологий. В Стратегиях, Доктринах этих стран отмечают важность подготовки специалистов в области информационной безопасности, и обучении кадров в других сферах.

В настоящее время ощущается острая нехватка кадров в области информационной безопасности во всех секторах экономики. Нет единых квалификационных требований к специалистам из данной области. Во многих странах организуют курсы дополнительной подготовки и повышения квалификации. В США, Франции и Великобритании существуют модели подготовки государственных кадров *Information Assurance* (IA).

Компетенции в области информационной безопасности необходимы не только специалистам ИТ сферы, но и специалистам уровня государственного управления, коммерческой или общественной организации, гражданам в личной жизни.

Государство заинтересовано в развитии образования в области информационной безопасности, а также в специалистах и квалифицированном персонале публичного и частного секторов, к которым, несомненно, относятся и экономисты. Подготовка таких специалистов с использованием новых методических подходов в системе высшего образования является актуальной задачей.

Описание ситуации в исследуемой области и идентификация проблемы исследования.

---

[11] *Портал о программах бакалаврита по всему миру.* Keystone [citat 23.12.2021]. Доступен: https://www.bachelorstudies.co.uk/BSc/Cyber-Security/

[12] *Официальный сайт Технологического института SANS*. SANS Technology Institute, © 2022 [citat 23.12.2021]. Доступен: https://www.sans.edu

Необходимость обеспечения безопасной передачи информации, сохранения ее целостности, конфиденциальности и доступности в любой сфере деятельности формирует тенденцию к включению вопросов защиты информации при изучении информационных технологий практически для всех направлений подготовки.

В области цифровой педагогики в Республике Молдова есть передовые исследования Gremalschi A.[13], Cabac V.[14], Canţer N. [15], Chiriac L., Globa A.[16], Afanas D.[17], Braicov A., Popov L. и многих других.

Большинство работ в Республике Молдова посвящены исследованиям различных направлений информационной безопасности, но не преподаванию этой дисциплины. Например, способы технической, правовой и криптографической защиты информации, освещены в работах Cojocaru I., Zgureanu A. Bădărău E., Guzun, M., Rotari A., Bragaru T., Briceag V., Popov L., Скринпник Н. и др. Защищена диссертационная работа Zgureanu A. в области физико-математических наук по теме «Securitatea informaţională şi metode de criptare bazate pe mulţimi de relaţii multi-are»[18]. Актуальные вопросы информационной безопасности ежегодно рассматривались в рамках Международной конференции "Securitatea informationala", проводимой Лабораторией информационной безопасности Молдавской Экономической Академии с 2004 по 2018 годы.

Об обучении информационной безопасности будущих педагогов с помощью разработанного электронного курса говорится в работе Великовой Т.[19]. Необходимость обучения экономистов информационной безопасности обоснована в статье[20]

---

[13] GREMALSCHI A. ş.a. Lecţii interactive pentru instruirea la distanţa în domeniul tehnologiei informaţiei şi a comunicaţiilor. In: *„Învăţământul universitar din Republica Moldova la 80 de ani", conf. şt. internaţ. Vol. 2: Probleme actuale ale didacticii matematicii, informaticii şi fizicii*. Chişinău: Univ de Stat din Tiraspol, 2010, pp. 219–230.

[14] CABAC, G. Individuaizarie formării în medii digitate prin construiria trazeelor individuale de instruire. In: *Formaria universitară în medii digitale: cercetări teoretico-experimentale*. Bălţi, 2015, p.197-236.

[15] CANŢER, N. *Didactica predării informaticii în învăţământul universitar: (Suport pentru prilegeri).* Chişinău: CEP USM, 2007. 65 p. ISBN 978-9975-70-470-0.

[16] CHIRIAC, L., GLOBA, A. Studierea informaticii în învăţământul preuniversitar prin prisma metodelor şi tehnicilor moderne de programare. In: *Studia Universitatis. Seria Ştiinţe ale educaţiei*. 2016, nr. 5(95). pp. 231-241. ISSN: 1857-2103.

[17] AFANAS Dorin. Fundamentele strategice privind dezvoltarea conceptului STEAM în cadrul laboratorului „Inteligența Artificială Creativă". In: *Conferința științifică international „Abordări inter/transdisciplinare în predarea științelor reale, (concept STEAM)" dedicată aniversării a 70 de ani de la nașterea profesorului universitar Anatol Gremalschi, vol.I* . Chișinău, 2021, p. 171-180. ISBN 978-9975-76-357-8.

[18] ZGUREANU, A. *Securitatea informaţională şi metode de criptare bazate pe mulţimi de relaţii multi-are*: tz. de doct. în ştiinţe fizico-matematice. Chişinău, 2011. 160 p.

[19] ВЕЛИКОВА, Т. Использование платформы дистанционного обучения при изучении дисциплины «Информационная безопасность». In: *Teoria şi practica administrării publice*. 20 mai 2013, Chișinău. Chișinău, Republica Moldova: Academia de Administrare Publică, 2013, pp. 449-452. ISBN 978-9975-4241-5-8.

[20] ОХРИМЕНКО, С. А., СКЛИФОС, К. Ф. Информационная безопасность для экономистов [online]. Лаборатория Информационной Безопасности [citat 18.06.2021]. Доступен: http://security.ase.md/publ/ru/pubru106/o_s.html

особенностью профессиональной деятельности, состоящей в активном применении информационных технологий и работой с ценными информационными ресурсами, подпадающими под понятие служебной тайны.

В школьном образовании в Республике Молдова научными работниками Cara A., Gremalschi A., Achiri I. по дисциплине «Информатика» в начальной школе рекомендована к изучению тема, позволяющая ученику «*демонстрировать ответственность за использование компьютера и защиту финансовой информации, хранящейся на компьютере*», а на уровне гимназических классов – тема «*Технические и организационные средства, используемые для защиты электронных финансовых транзакций*»[21, с.7-8].

Все эти исследования свидетельствуют о важности формирования и развития компетенций в области информационной безопасности на всех этапах обучения в соответствии с Концепцией информационной безопасности РМ от 21.12.2017.

В Румынии много серьезных научных работ в области практических подходов к обучению основам информационной безопасности авторов Scripcariu L., Bogdan I., Ploteanu N.[22], Patriciu V. V., Mihai I. C.[23], Stanciu V., Tinca A.[24], Udroiu M.[25], Sarcinschi A.[26] и других. Многие авторы считают, что в настоящее время недостаточно готовить в профессиональной школе только специалистов в области ИТ, которые занимаются вопросами информационной безопасности в организациях. Необходимо в университетах, не связанных с информационными технологиями, включать в процесс обучения специфические аспекты информационной безопасности (и соответствующие навыки в области информационных технологий), чтобы должным образом подготовить студентов к будущему. «*Например, …для студентов-медиков вопросы информационной безопасности должны быть включены в учебную программу, чтобы подготовить их к деятельности в области электронного здравоохранения. Для студентов-юристов аспекты*

[21] CARA, Angela, GREMALSCHI, Anatol, ACHIRI, Ion. Integrarea Educaţiei financiare în curricula naţionale. In: *Univers Pedagogic*. 2016, nr. 2(50), pp. 3-9. ISSN 1811-5470.
[22] PLOTEANU, N. Matricea infractorilor computaţionali . In: *Anale ştiinţifice ale Academiei „Ştefan cel Mare" a MAIRM: ştiinţe juridice.* 2003, nr. IV, pp. 253-260. ISSN 1857-0976.
[23] MIHAI, I. C. *Securitatea informațiilor*. Craiova: Editura Sitech, 2012. p. 317. ISBN 978-606-11-29203-4.
[24] STANCIU, V., TINCA, A. *Securitatea informației. Principii si bune practici*. Ediția a doua. Bucuresti : Editura ASE, 2015. 232 p. ISBN 978-606-505-902-3.
[25] UDROIU, M. POPA, C. *Securitatea informaţiilor în societatea informaţională*. Bucureşti: Editura Universitară, 2010. p. 402. ISBN: 978-973-749-831-1.
[26] SARCINSCHI, A. *Vulnerabilitate, risc, ameninţare. Securitatea ca reprezentare psihosocială*. Bucureşti: Editura Militară, 2009. p. 248. ISBN: 978-973-32-0739-9.

информационной безопасности должны быть представлены так, чтобы они понимали техническую и юридическую составляющую»[27].

Профессор немецкого Университета Бундесвера в Мюнхене Udo Helmbrecht, доктор теоретической физики, исполнительный директор Европейского агентства кибербезопасности ENISA (2009-2019 гг.) пишет, что «*..в цифровом обществе …безопасность нашей информации имеет основополагающее значение, и по мере цифровой трансформации наша жизнь становится все более подверженной угрозам кибербезопасности. Новые вызовы информационной безопасности и кибербезопасности — это ответы на развивающиеся новые технологии и новые бизнес модели*». Ученый ключевым риском информационной безопасности называет «всё возрастающую сложность систем», а также определяет технические, социальные, этические и правовые риски киберпространства. Подготовка в университетах играет важную роль, так как в бизнес кругах растет осознание важности дисциплины «Информационная безопасность» и руководители компании все больше внимания уделяют кибербезопасности [28, с. 35].

В России вопросы обучения информационной безопасности на различных уровнях образования и различных направлениях подготовки освещены в диссертационных работах Алтуфьевой А. А., Боярова Е. Н., Ломаско П. С., Матвеева Н.А., Димова Е. Д., Тановой Э. В., Синицына Д. С., Малых Т. А., Серебряника Е. Э. и др. Работы Полякова В.П., Абиссовой М. А., Горбунова А. И. посвящены проблемам формирования компетенций в области информационной безопасности у студентов социально-экономических специальностей.

Изучена специализированная литература по различным направлениям обеспечения информационной безопасности: техническим, криптографическим, физическим, правовым и психологическим.

Технологические аспекты области информационной безопасности рассмотрены в большом количестве работ зарубежных и отечественных исследователей. Перечислим только некоторых из них: Schneier Bruce [29], Adams C.M., Anderson R. J. [30], Smith Richard E., Олифер, Молдовян, Андрончик А.Н., Богданов В. В.; Емельянова Н. З., Партыка Т. П.,

---

[27] GĂBUDEANU, L. Propunere pentru abordări practice în educația privind securitatea informației. In: *Securitatea cibernetică - Provocări și perspective în educație*, ROMÂNIA, 2020. p.183-190. ISBN 978-606-11-7675-5.

[28] HELMBRECHT, U. Cybersecurity from a University Perspective In: *Securitatea cibernetică - Provocări și perspective în educație*, ROMÂNIA, 2020. p.29-38. ISBN 978-606-11-7675-5.

[29] Шнайер, Б. *Практическая криптография, 2-е издание: протоколы, алгоритмы, исходные тексты на языке Си.* Москва: Триумф, 2002. 610 с.

[30] ANDERSON, R. J. Searching for the Optimum Correlation Attack. In: *Fast Software Encryption*, 1994. pp. 137-143. ISBN 978-3-540-60590-4.

Попов И. И.; Игнатьев В. А.; Каторин Ю. Ф., Разумовский А. В., Спивак А. И.; Платонов В. В.; Пролетарский А. В., Суворов А. М., Смирнова Е. В., Руденков Н. А.; Торокин А. А., Ярочкин В. И.; Романец; Малюк А. А., Пазизин С. В., Погожин Н. С.; Нестеров С. А. Бакланова В. В.; Мельникова В. П., Клейменова С. А., Петракова А. М.; Шаньгина В. Ф.; Зима В. М., Молдовяна А. А. и другие.

Правовые аспекты информационной безопасности рассмотрены в работах Anderson R., Поляковой Т. А., Стрельцова А. А., Пожарского В. Н., Минаева В. А., Тарапановой Е. А., Фролова Д. Б., Скрыль С. В., Сычева А. М., Коробец Б. Н., Вайц Е. В., Грачева Ю. В., Астрахова А. В. и других.

Психологические аспекты возникновения угроз информационной безопасности и этико-психологические методы по обеспечению ее защиты рассмотрены в работах Шмидт Э. и Коэн Д.[31], Кузнецова М. В.[32], Кефели И. Ф. и Юсупова Р.М. [33], Челноков В. В. [34] и других ученых.

Несмотря на разносторонность выполненных исследований и их несомненную теоретическую и прикладную значимость, работы не исчерпывают проблему определения методов, средств, эффективности обучения будущих экономистов основам информационной безопасности. Анализ литературных источников выявил недостаточную разработанность методологии обучения основам информационной безопасности будущих экономистов, которая позволила бы сформировать компетенции в области информационной безопасности, проанализировать обученность студентов по дисциплине, оценить эффективность применения методов и средств в процессе обучения.

Анализ содержания стандарта и программ подготовки бакалавров по направлению подготовки «Экономика» в учебных заведениях показывает, что эта подготовка сводится, как правило, к изучению технических либо криптографических способов защиты информации.

При этом не рассматриваются:

1) организационно-правовые средства защиты информации;

2) морально-этическое направление обеспечения информационной безопасности;

---

[31] ШМИДТ, Э., КОЭН, Д. *Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств.* Москва: ООО «Манн, Иванов и Фербер», 2013. 368 с. . ISBN 978-5-91657-824-9.

[32] КУЗНЕЦОВ М.В., СИМДЯНОВ, И.В. *Социальная инженерия и социальные хакеры*. Санкт-Петербург: БХВ-Петербург, 2007. 368 с. ISBN 5-94157-929-2.

[33] КЕФЕЛИ, И. Ф. ЮСУПОВА, Р. М. *Информационно-психологическая и когнитивная безопасность.* Санкт-Петербург: ИД «Петрополис», 2017. 300 с. ISBN 978-5-9676-0895-7.

[34] ЧЕЛНОКОВ, В. В. *Психологические аспекты обеспечения Информационной безопасности*. Екатеринбург: УрГУ, 2008. 47 с.

3) практико-ориентированные задания для формирования практических навыков обеспечения информационной безопасности в профессиональной деятельности экономистов.

Такой подход не позволяет в должной мере сформировать комплексное представление об информационной безопасности и развить цифровые компетенции в этой области.

С точки зрения системного подхода в процессе обучения информационной безопасности необходимо изучить основные понятия, угрозы, каналы утечки, организационные, правовые, физические, программные, технические, морально-этические средства защиты информации, процессы идентификации и аутентификации, основы криптографии, алгоритмы хеширования и электронно-цифровой подписи, получить навыки защиты информации для будущей профессиональной деятельности. С учетом широты тематики и ограничения аудиторного времени на изучение дисциплины большое значение приобретают методы и средства обучения, применение информационных технологий, в том числе интернет-технологий, в процессе преподавания, оценивания результатов деятельности, активизации самостоятельной работы студентов.

Большинство исследователей пишут о недостаточной разработанности методологических подходов к обучению основам информационной безопасности студентов нетехнических специальностей.

Различный уровень начальных знаний студентов, приобретенных в рамках школьного курса «Информатика», постоянное расширение диапазона современных информационных технологий, недостаточность специализированной литературы и методических материалов, понятных и необходимых в будущей профессиональной деятельности, ограниченное количество часов в рамках учебного плана, – все это усложняет обучение основам информационной безопасности и выдвигает определенные требования к методической системе подготовки будущих экономистов в данной области.

Выше сказанное позволяет выделить следующие **противоречия** между:

– требованиями, возникающими к специалистам экономического профиля при работе с ценной информацией организации с точки зрения обеспечения информационной безопасности, и необходимостью совершенствования процесса подготовки студентов экономических специальностей для формирования необходимых компетенций в области информационной безопасности;

– требуемыми практическими навыками, которыми должен владеть экономист при работе с ценной информацией и педагогическими технологиями формирования этих

навыков у студентов в процессе обучения информационным технологиям;

– существующим большим разнообразием методических и учебных материалов по техническим, программным, криптографическим методам защиты и необходимостью разработки учебно-методического комплекса для проведения теоретических и практических занятий в процессе формирования в вузе у будущих экономистов компетенций в области информационной безопасности;

– сложившейся практикой оценивания уровня обученности с одной стороны и применением балльно-рейтинговой системы оценки результатов и эффективности процесса обучения дисциплине «Информационная безопасность».

Указанные противоречия породили **проблему исследования**, заключающуюся в определении теоретических и методологических основ повышения эффективности и качества изучения технологий защиты информации и информационной безопасности с перспективы интернет-технологий и кибернетического подхода в рамках формирования профессиональных компетенций будущих специалистов финансово-экономической сферы, востребованных на рынке труда.

Объект исследования представляет собой внедрение новых интернет-технологий в учебный процесс изучения университетского курса «Информационная безопасность».

Цель исследования состоит в теоретическом обосновании, разработке и проверке экспериментальным путем педагогической модели обучения будущих специалистов финансово-экономической сферы технологиям защиты информации и информационной безопасности посредством интернет-технологий.

Основные гипотезы исследования. Если:

- будет научно обосновано внедрение информационных технологий, в том числе интернет-технологий, в процесс изучения технологий защиты информации и информационной безопасности для будущих специалистов в финансово-экономической сфере;
- будут разработаны и усовершенствованы учебно-методические комплексы по университетской дисциплине «Информационная безопасность» с внедрением интернет-технологий;
- будет разработана педагогическая модель изучения технологий защиты информации и информационной безопасности для будущих специалистов финансово-экономической сферы с использованием интернет-технологий, в которой будут учтены требования рынка труда и основные педагогические и дидактические принципы;

- будет разработана, описана и экспериментально подтверждена методология обучения технологиям обеспечения информационной безопасности путем внедрения информационных технологий, в том числе интернет-технологий, с точки зрения личностно-ориентированного обучения.

тогда это позволит сделать эффективным и качественным изучение технологий защиты информации и информационной безопасности с точки зрения интернет-технологий в рамках профессиональной подготовки студентов финансово-экономического направления подготовки.

Задачи исследования:

1) сформулировать методические принципы и подходы, необходимые для проектирования дидактической системы обучения будущих специалистов финансово-экономической сферы дисциплине «Информационная безопасность»;

2) концептуализировать показатели оценивания, критерии и дескрипторы достижений для обеспечения эффективности учебного процесса при изучении информационной безопасности;

3) разработать педагогическую модель обучения будущих специалистов финансово-экономической сферы дисциплине «Информационная безопасность», отражающую содержательную часть дисциплины и методическую систему формирования компетенций в области информационной безопасности;

4) разработать учебно-методический комплекс дисциплины «Информационная безопасность» с использованием информационных технологий, в том числе интернет-технологий;

5) разработать, внедрить и экспериментально проверить эффективность спроектированной педагогической модели и оптимизировать учебный процесс посредством использования новых информационных технологий.

В процессе реализации целей дидактически-научного исследования основное внимание уделялось следующим **методам исследования:**

• теоретические методы: научные исследования и документация; анализ; сравнение; синтез; обобщение; систематизация; проектирование, описание и педагогическое моделирование;

• экспериментальные методы: педагогический эксперимент; индивидуальные проекты; наблюдение, опрос, тестирование, анализ и оценивание;

• методы анализа: статистическая обработка экспериментальных данных; количественный и качественный анализ результатов, полученных экспериментально.

Научная новизна и оригинальность исследования состоит в концептуальном обосновании педагогической модели проектирования и реализации вузовской дисциплины «Информационная безопасность» посредством внедрения интернет-технологий.

Научная проблема, решенная в исследовании заключается в определении теоретико-методологических основ обеспечения эффективности изучения вузовской дисциплины «Информационная безопасность», что привело к теоретическому обоснованию и разработке педагогической модели преподавания-обучения-оценивания университетского курса посредством интернет-технологий, ориентированных на процесс формирования профессиональных компетенций будущих специалистов финансово-экономической сферы.

Теоретическая значимость исследования заключается в исследовании и оценивании применения интернет-технологий в процессе формирования и развития профессиональных компетенций в области информационной безопасности у будущих специалистов в финансово-экономической сфере с помощью разработанной педагогической модели.

Практическая значимость исследования определяется эффективной реализацией разработанной педагогической модели и использованием разработанной методики обучения в процессе обучения вузовской дисциплине «Информационная безопасность» студентами финансово-экономической сферы посредством применения интернет-технологий, с целью формирования и развития профессиональных компетенций в области защиты информации и информационной безопасности.

Кроме этого в процессе исследования разработаны:

1) учебно-методический комплекс по дисциплине «Информационная безопасность», включающий в себя краткий курс лекций, сборник заданий к выполнению лабораторных работ, система тестовых заданий для определения уровня обученности студентов экономических специальностей основам информационной безопасности;

2) разработаны и интегрированы в информационную образовательную среду вуза электронное учебное пособие «Информационная безопасность», сетевое электронное издание методических указаний к выполнению лабораторных работ, сетевое электронное издание тестовых заданий по дисциплине.

Внедрение результатов исследования было осуществлено в образовательный процесс Тираспольского Государственного Университета (г. Кишинэу), Бендерского

политехнического филиала Университета им. Т. Г. Шевченко, Тираспольского филиала Московской академии экономики и права, Тираспольского филиала «РОСНОУ».

Апробация научных результатов. Результаты исследования были представлены на заседании кафедры «Информатики и информационных технологий» Тираспольского государственного университета, ежегодных отчетах Școala Doctorală „Științe ale Educației" a Parteneriatului instituțiilor de învățământ superior Universitatea de Stat din Tiraspol, Universitatea de Stat „Bogdan Petriceicu Hașdeu" din Cahul și Institutul de Științe ale Educației, а также в 4 национальных научно-методических конференциях (2018-2022), 7 национальных научно-методических конференциях с международным участием (2018-2021 гг.) и 13 международных научно-методических конференциях (2017-2021 гг.) (Приложение 16). Публикации материалов по теме диссертационного исследования представлены: в 3 статьях в журналах категории "B" *Acta et commentationes. Ştiinţe ale Educaţiei* и *Revista Univers Pedagogic* [20, 61, 119], в 2 статьях в журналах категории "C" *Revista de Stiinţe Socioumane* и *Acta Et Commentationes* (2018) [60, 68], в рецензируемом журнале из списка ВАК РФ *Мир университетской науки: культура, образование* [156].

Методические указания «Информационная безопасность. Защита офисных документов» и «Информационная безопасность: Курс лекций для экономистов» были одобрены на Совете Факультета Физики, Математики и Информационных Технологий Тираспольского Государственного Университета в 2019 году.

Содержание диссертационной работы.

Во **Введении** аргументирован выбор темы исследования; обозначены актуальность и значимость темы; сформулирована цель исследования, исходя из которой, определены задачи его проведения. Перечислены методы исследования; описаны, в соответствии с областью исследования, новизна и оригинальность, теоретическая и практическая значимость; обосновано практическое внедрение результатов.

Первая глава «Психолого-педагогические основы обучения технологиям защиты информации в системе высшего профессионального образования будущих экономистов» посвящена анализу информационной безопасности как новой области знаний, ее месту в формировании цифровой грамотности. Проведено исследование стандартов и учебных планов подготовки экономических кадров в данной области в разных странах. Обоснована необходимость пересмотра применяемых дидактических приемов в преподавания информационной безопасности будущим экономистам.

Во второй главе «Педагогическая модель и методология обучения информационной безопасности студентов экономических специальностей»

смоделирован процесс обучения информационной безопасности с точки зрения системного подхода**.** Рассмотрены междисциплинарные связи, проявляющиеся в процессе «преподавание – обучение – оценивание» дисциплины «Информационная безопасность». Обоснована и представлена педагогическая модель обучения данной дисциплине будущих специалистов финансово-экономической сферы. Рассмотрена методология использования разработанной педагогической модели в процессе обучения дисциплине «Информационная безопасность».

В третьей главе «Экспериментальное обоснование эффективности педагогической модели и методологии ее применения» проанализированы виды педагогических исследований**,** описана организация, проведение и результаты педагогического эксперимента, а также реализован математико-статистический анализ результатов исследования.

Ключевые слова: информационная безопасность, балльно-рейтинговая система оценивания, педагогическая модель, образовательный веб-квест, самостоятельная работа студентов, интернет технологии, педагогический эксперимент, кибернетический подход, системный подход.

1 ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЕ ОСНОВЫ ОБУЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ ЭКОНОМИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

1.1 Информационная безопасность как междисциплинарная отрасль знаний

Вопросами защиты информации начали заниматься еще в Древнем Египте, Греции, в Средние века, в Эпоху Возрождения, во время двух мировых войн XX века. Но бурное развитие отрасли знаний «Информационная безопасность» началось с развитием компьютерной техники в середине XX –го века. Переход в эру Четвертой промышленной революции, связанный с цифровой трансформацией экономики, обусловил всеобщую информатизацию, информационные технологии прочно вошли в жизнь современного общества, проникли во все сферы хозяйственной деятельности. Увеличилось количество и интенсивность угроз информационной безопасности, но и появились новые средства защиты информации. На сегодняшний день невозможно представить ни одну отрасль экономики не применяющую информационные технологии, и, соответственно, везде осуществляются атаки на информационные активы.

С исторической точки зрения проблемами защиты информации начинали заниматься с Древних времен. Человек вскоре после того, как изобрел знаки для хранения и передачи сообщения, пожелал скрыть информацию от тех, кому она не предназначалась.

В учебнике по информационной безопасности под редакцией Ященко В. В., отмечено, что «*свой след в криптографии оставили многие хорошо известные исторические личности*», такие как спартанский полководец Лисандр, Цезарь, математик Д. Кардано, король Генрих IV, кардинал Ришелье, Петр Великий и многие другие [35, с. 12-13].

В книге Соболевой Т. А. описана история возникновения российской криптографической службы со времен Петра Великого и до начала Второй мировой войны. Считается, что «*наиболее ранней из известных по древнерусским памятникам письменности систем тайнописи является система «иных» письмен*», при котором происходила замена букв кириллицы на буквы других алфавитов: «*глаголицы, греческого, латинского, пермской азбуки*» [36, с. 24] .

Наиболее обширный исторический экскурс в области криптографии представлен в

---

[35] ЯЩЕНКО, В. В. и др. *Введение в криптографию*. 4-е изд. Москва: МЦНМО, 2012. 348 с. ISBN 978-5-4439-0026-1.

[36] СОБОЛЕВА Т.А. *История шифровального дела в России*. Москва: ОМА-ПРЕСС-Образование, 2002. 511 с. ISBN 5-224-03634-8.

работе David Kahn “Codebreakers. The story of Secret Writing” (New York: Macmillan, 1967), в которой интересно описана история криптографии от Древних времен до наших дней. Автор приводит как пример первого зашифрованного сообщения: «*Однажды, почти четыре тысячи лет тому назад, в городе Менат-Хуфу на берегу Нила, один опытный писец нарисовал иероглифы, рассказавшие историю жизни его господина – и сделав это, он стал родоначальником документально зафиксированной истории криптографии...*» [37], с. 64-.65.

История защиты информации с Древних времен до наших дней, переработанная автором на основе книги David Kahn и Соболевой Т. А., представлена в таблице 1.1.

Таблица 1.1. Хронология развития знаний в области защиты информации

Моноалфавитные шифры (3 тыс. до н. э. - VIII в. н. э.)	Индия, Месопотамия, Древний Египет	до XX века до н.э.	Замена гласных букв согласными в древнеиндийских письменах. Месопотамия: рецепт на глиняной табличке с цифрами вместо имен. История жизни фараона, написанная на камнях иероглифами, шифры замены
	Древняя Греция, Китай	XIX-VI века. до н.э.	Приемы и алгоритмы шифрования информации для сохранения ее в секрете и безопасной передаче описаны в трудах Лисандра, Сцитала, Полибия, Энея, Пифагора, Платона, Аристотеля, Цезаря и многих других
	Древний Рим	V в. до н. э. -IV в. н. э.	
Полиалфавитные шифры (IX - XIX века)	Средние века	V - XVI вв.	Книга о большом стремлении человека разгадать загадки древней письменности (855). Ал-Кинди «Манускрипт о дешифровке криптографических сообщений» (IX век). Ас-Сули «Адаб аль-Куттаб» («Руководство для секретарей») инструкции по шифрованию записей о налогах (X в.). Шихаб аль-Кашканди в «Шауба ал-Аща» (14-томной энциклопедии) в разделе «Относительно сокрытия в буквах тайных сообщений» описаны 7 способов шифрования, таблица частотности букв арабского языка на основе текста Корана (1412). Альберти Леон Баттист «Трактат о шифрах» (1466), изобрел шифровальный диск. Абат Тритемиус (1508) Трителлий И.. Джероламо Кардано изобрел шифровальное устройство «поворотная решетка» (1550). Джованни Белазо предложил применять «лозунг», или пароль (1553). Джованни Батиста де ла Порта из Неаполя «О тайной переписке» (1563). Блез де Вижжинер «Трактат о шифрах» (1586) и др.
	Новое время, Просвещение	XVII XVIII XIX	«Эра черных кабинетов» - возникновение в Королевстве Великобритания, Франции, Австро-Венгрии, Германии, России служб по дешифровке. Джефферсон Т. – третий президент США – изобрел шифрующий цилиндр (1790); Чарльз Уитстон изобрел шифровку биграммами (1854); Этьен Базери создал цилиндр Базери (1891)

[37] KAHN, D. *Codebreakers. The story of Secret Writing*. New York: Macmillan, 1967, 473 с.

Электромеханические устройства (начало XX-го века)	Новейшее время: Мировые войны XX-го века, III и IV Промышленные революции	XX	Жильбер Вернам создал первую практически используемую шифровальную машину (1917). Эдвард Хеберн роторная криптографическая машина «Энигма» (1923). Алан Тьюринг создал ЭВМ «Колосс» для взлома шифров «Энигмы». Клод Шенон «Математическая теория связи» (1948). Диффи У. и Хеллман М. Э. «Новые направления в криптографии» (1979); Стандарт 5200.28 «Trusted Computing System Evaluation Criteria» (TCSEC) (Оранжевая Книга Министерства обороны США, 1983). Алгоритмы симметричного и ассиметричного шифрования
Современная криптография, право, этика, стандарты, техника (с середины XX-го века)		XXI	Защита интернет-пространства (КНР, 2000); Стратегия ИБ (2003, США); Доктрины ИБ и законы о защите информации во всех развитых государствах; Международные Стандарты в области ИБ, Кодексы профессиональных сообществ по этике и т.д.

Из таблицы 1.1 видно, что изначально конфиденциальность информации сохраняли путем ее сокрытия с помощью криптографии. С созданием в середине 20-го века ЭВМ появились новые способы хранения, передачи и обработки данных, колоссально усложнились криптографические алгоритмы, появились новые способы защиты информации: технические, программные, организационные, правовые и этические.

Таким образом, понятно, почему информационная безопасность, будучи частью дисциплин информационного цикла, является в то же время междисциплинарной наукой, пересекающейся с математикой, физикой, юриспруденцией, экономикой, психологией, социологией, историей и другими областями знаний.

Приведем некоторые примеры понимания информационной безопасности в контекстах различных областей знаний.

Активное применение информационных технологий в противоправном порядке поспособствовали возникновению нового направления – информационного права. О его значении в разрешении противоречий между, созданной после третьей промышленной революции, информационной сферы с существующей биосферой пишет профессор Рассолов И. М.: «*Это может приводить к конфликтам в социуме и ставить перед современной правовой системой, а также научной доктриной многочисленные правовые проблемы (например, проблему идентификации лиц, борьбы с кибернетической преступностью, внедрения новых «живых» технологий, оборота генетической информации, борьбы с глобальным потеплением и др.)*»[38, с. 92]. Будущих специалистов финансово-экономической сферы необходимо знакомить с правовыми проблемами,

[38] РАССОЛОВ, И. М. Правовое регулирование в информационной сфере. В: *Актуальные проблемы российского права*. 2016, № 4(65), с. 92-96. ISSN 1994-1471.

которые могут возникнуть в процессе хранения, обработки и передачи информации.

Все более частое применение методов социальной инженерии для получения конфиденциальной информации, информационно-психологического воздействия на личность потребовали изучения социальных и психологических аспектов в области информационной безопасности. Еще со времен Древней Греции и Рима были востребованы люди, которые применяли знания об обществе и предвидение возможных результатов для того, чтобы вводить в заблуждение и убеждать в своей правоте собеседника. В современном мире подходы прикладной социологии стали применять в информационных системах для манипуляции огромными «массами пользователей, побуждая их поступать по заранее разработанному сценарию». Ламинина О. Г. пишет, что «*методы социальной инженерии способны обойти самые мощные системы информационной безопасности*», т.к. «*они воздействуют непосредственно на самое слабое место в системе информационной безопасности – на пользователя*» [39, с. 2-3].

О том, как на практике применяются методы социально-психологического воздействия, изложено в научно-популярных книгах «Искусство обмана» (Кевин Митник и Вильям Л. Саймон, 2004), «Социальная инженерия и социальные хакеры» (Кузнецов М. В. и Симдянов И. В, 2007[40]). О противодействии социальной инженерии вышла книга Кевина Митника «Искусство быть невидимым: как сохранить приватность в эпоху Big Data» (2019)[41]. Обучение противодействию методам социальной инженерии необходимо включить в профессиональную подготовку будущих специалистов финансово-экономической сферы.

Перевод многих бизнес-процессов в цифровую среду вызвал потребность в применении экономических законов и методов анализа при соотнесении затрат на обеспечение информационной безопасности и ценности информации. Профессор инженерии безопасности Кембриджского университета Anderson Ross отмечает, что информационная безопасность, начиная с 2000 годов, перестала быть просто технической дисциплиной с математической составляющей в виде криптографии, а стала дисциплиной, находящейся на стыке технологий, экономики и психологии.

---

[39] ЛАМИНИНА, О. Г. Возможности социальной инженерии в информационных технологиях. В: *Гуманитарные, социально-экономические и общественные науки.* 2017, №2. ISSN 2220-2404.

[40] КУЗНЕЦОВ, М.В., СИМДЯНОВ, И. В. *Социальная инженерия и социальные хакеры*. Санкт-Петербург: БХВ-Петербург, 2007. 368 с. ISBN 5-94157-929-2.

[41] МИТНИК, К. *Искусство быть невидимым: как сохранить приватность в эпоху Big Data*. Москва: Эксмо, 2019. 464 с. ISBN 978-5-04-094446-0.

Ученый пишет: «*управление информационной безопасностью гораздо более глубокая и политическая проблема, чем это обычно осознается; … многие упрощенные технические подходы обречены на провал. Пришло время для инженеров, экономистов, юристов и политиков попытаться выработать общие подходы*»[42] .

Информационная безопасность в настоящее время стала частью экономической безопасности личности, организации и государства. На уровне личности, персональные данные могут стать предметом торговли, а впоследствии нанести экономический и репутационный ущерб. На уровне организации «*утечка информации сопоставима с физической утратой капитала*». На уровне государства становится необходимым поддержание информационной безопасности, так как «*информационная сфера оказывает прямое влияние на систему международных экономических отношений*» [43].

Множество научных публикаций в области информационной безопасности связаны с криптографией, которая являясь разделом математики, стала одним из самых мощных способов защиты информации от нарушения конфиденциальности, целостности и доступности. Atanasiu Adrian пишет: «*криптография является компонентом гораздо более широкой области, называемой информационной безопасностью*»[44, с.5].

В 70-х годах XX-го века криптографические методы защиты дополнились исследованиями в области квантовой физики: предложена возможность создания фундаментально надежного и безопасного способа передачи секретного ключа по квантовому каналу связи. «*Теория квантовой информации кардинально изменит современные взгляды научного сообщества на основу системы информационной безопасности*»[45, с.14] .

Тесная взаимосвязь между физикой и информационной безопасностью обусловлена также физической природой хранения, передачи и обработки информации.

Как видим, дисциплина «Информационная безопасность» выходит за рамки технических и криптографических средств защиты, можно сказать, является объектом

---

[42] ANDERSON, R. Why Information Security is Hard An Economic Perspective. В: *17th Annual Computer Security Applications Conference. December 10-14, 2001. New Orleans, Louisiana.* [online]. 2001 [citat 05.08.2021]. Доступен: https://www.acsac.org/2001/papers/110.pdf

[43] ПОПОВА, С. В., ФЕДОРИНОВ, В. Е. Экономические аспекты доктрины информационной безопасности. В: *Воздушно-космические силы. Теория и практика*. 2018, № 5 (5), с.17-24. ISSN 2500-4352.

[44] ATANASIU, Adrian. *Securitatea Informației.* Vol. 1 (Criptografie). Cluj: Editura INFODATA, 2012. 237 p. ISBN 978-973-1803-16-6.

[45] АКТАЕВА, А., БАЙКЕНОВ, А., ГАЛИЕВА, Н., АСАНОВА, К., БАЙМАН, Г., ШАТЕНОВА, Г. Квантовая информация: методы защиты информации. В: *Современные информационные технологии и ИТ-образование.* Том 12. 2016, № 2, с. 6-14. ISSN 2411-1473.

междисциплинарных исследований на стыке компьютерных наук, электроники и электротехники, права, математики, физики, истории, этики, психологии и социологии.

Междисциплинарность в принципе становится современной тенденцией в образовании, необходимой для понимания процессов и явлений, происходящих в обществе. Книгин А. Н., рассматривая проблему междисциплинарности с философской точки зрения, говорит о необходимости формирования междисциплинарного мышления с помощью овладения знаниями в рамках конкретной дисциплины, дополняя и насыщая ее «приёмами междисциплинарной подачи материала, формирующими междисциплинарное мышление» [46, с. 18].

Особое место информационной безопасности, как отрасли знаний, позволило занять то обстоятельство, что информация стала одним из ценнейших ресурсов наряду с полезными ископаемыми [47]. Компьютер может использоваться не только как мощное средство оптимизации и повышения эффективности, но и как средство совершения противоправных действий. Угрозы информационной безопасности стали постоянными рисками для всех организаций, независимо от отрасли, в которой они функционируют. Будущие специалисты финансово-экономической сферы должны быть осведомлены о том, какую информацию необходимо защищать в организации, от кого защищать и как защищать.

На современном этапе развития общества информационная безопасность – это больше, чем просто проблема решаемая специалистами в области информационных технологий, – это стратегический инструмент, способствующий развитию бизнеса. В Отчете ВЭФ «*Принципы управления киберрисками*» отмечено, что жизненно важно пересмотреть модели управления киберрисками, т.к. «*эффективная модель информационной безопасности напрямую способствует сохранению финансовых ресурсов и созданию новых возможностей для предприятия и общества в целом»* [48, с. 7].

Понимание важности создания и поддержания эффективной модели информационной безопасности в организации противостоит неоднозначности терминологии в области обеспечения защиты данных.

Научно-технический прогресс, начавшийся в середине 50-х годов XX-го века, был

---

[46] КНИГИН А. Н. Междисциплинарность: основная проблема. В: *Вестник Томского государственного университета. Философия. Социология. Политология*. 2008, №3(4), с.14-20. ISSN 2311-2395.

[47] СТОУНЬЕР, Т. Информационное богатство: профиль постиндустриальной экономики. В: *Новая технократическая волна на Западе*. Москва: Знание, 1986. с. 392 – 409.

[48] Отчет ВЭФ «Principles for Board Governance of Cyber Risk» [online]. *Сайт Всемирного Экономического Форума (ВЭФ),* 2021 [citat 07.07.2021]. Доступен: http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf

связан с созданием компьютеров, применением атомной энергии и других прорывных идей в науке, технологии и производстве. В это же время начали говорить о безопасности данных. Исторически сложилась терминология: «*безопасность данных*», «*компьютерная безопасность*», «*безопасность информации*», «*информационная безопасность*», «*защита информации*», «*сетевая безопасность*», «*кибербезопасность*»[49, с. 28].

В контексте «сетевая безопасность» и «кибербезопасность» трактуется защита национальных интересов развитых стран, таких как США, государства ЕС и другие. Под сетевой безопасностью понимается защищенность телекоммуникационных сетей на национальном и глобальном уровнях. Кибербезопасность рассматривается как защищенность от внутренних и внешних угроз киберпространства, а именно: взаимосвязанной сети инфраструктур, использующих различные информационные технологии. Понятие «*информационная безопасность*» на международном уровне впервые было использовано в 1998 году в резолюции Генеральной Ассамблеи ООН о достижениях в сфере информатизации и телекоммуникации в контексте международной безопасности. Можно считать, что «*сетевая безопасность*» является составляющей понятия «*кибербезопасность*», а оно, в свою очередь, входит в понятие «*информационная безопасность».*

Рис. 1.1. Соотношение понятий «сетевая безопасность», «кибербезопасность» и «информационная безопасность» [50, с. 12].

* По Стрельцову А. А., доктор (2016)

Согласимся со схемой, предложенной членом-корреспондентом Академии криптографии РФ Стрельцовым А. А., что эти понятия взаимосвязаны, и

[49] КУРИЛО, А. П., МИЛОСЛАВСКАЯ, Н. Г., СЕНАТОРОВ, М. Ю., ТОЛСТОЙ, А. И. *Основы управления информационной безопасностью.* 2-е изд. Москва: Горячая линия-Телеком, 2014. 244 с. ISBN 978-5-9912-0361-6.

[50] ПОЛЯКОВА, Т. А., СТРЕЛЬЦОВ, А. А. *Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры*. Москва: Юрайт, 2016. 325 с. ISBN 978-5-9916-6799-9.

информационную безопасность надо трактовать шире, чем кибербезопасность, фокус которой скорее сконцентрирован на обеспечении безопасности информации и технических сред передачи данных. Далее будем рассматривать термин «информационная безопасность».

В настоящее время не существует ясного и точного определения, отражающего сущность термина «информация», соответственно не выработано четкого и однозначного определения понятия «информационная безопасность». Рассмотрим значение этого термина в нормативных актах, международных стандартах и научной литературе. Понимание этих аспектов непосредственно позволит сформулировать тематику дисциплины, а также разработать эффективную методику преподавания основ информационной безопасности будущим специалистам финансово-экономической сферы.

Понятие «информационная безопасность» в нормативных актах

В Республике Молдова в официальных документах «Стратегия информационной безопасности Республики Молдова на 2019–2024 годы», «Постановление Правительства Республики Молдова № 811 от 29.10.2015 о Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы» используется термин «кибербезопасность». Под кибербезопасностью в нормативных актах Республики Молдова понимают «*нормальное состояние, возникшее вследствие применения комплекса проактивных и реактивных мер, посредством которых обеспечивается конфиденциальность, целостность, доступность, достоверность и невозможность отказа в доступе к информации в электронном формате, информационных систем и ресурсов, государственных и частных услуг в киберпространстве*» [51].

Европейский парламент и Совет Европейского Союза в Регламенте относительно Агентства Европейского Союза по сетевой и информационной безопасности (ENISA – European Union Agency for Cybersecurity) определяет, что нарушение электронных коммуникаций, инфраструктуры и услуг «*может нанести значительный физический, социальный и экономический ущерб, что подчеркивает важность мер по повышению защиты и устойчивости, направленных на обеспечение непрерывности критически важных услуг»*. Поэтому под безопасностью электронных коммуникаций, инфраструктуры и услуг, понимается их целостность, доступность и

[51] Постановление Правительства Республики Молдова о Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы: № 811 от 29.10.2015. В: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 306-310, 905.

конфиденциальность[52, ст. 1] .

При этом в ЕС один из самых серьезных подходов к защите персональных данных. В мае 2018 года введен в действие General Data Protection Regulation (GDPR) – Общий регламент по защите данных ЕС 2016/679, имеющий экстерриториальный принцип действия, т.е. обязательный к применению любой компанией (независимо от местонахождения), работающей с персональными данными жителей ЕС. При этом в Европейском Союзе нет единой концепции информационной безопасности. В каждой стране свои, иногда противоречивые, подходы, связанные с информационной безопасностью.

В американских правовых документах чаще применяется термин «кибербезопасность». США, являясь пионером создания интернет технологий и организационных структур по защите компьютерной информации, наиболее часто изменяют доктринальные документы по кибербезопасности государства.

В федеральном законодательстве США определяется, что информационная безопасность включает в себя защиту информации и информационных систем от различных угроз, таких как нарушение: 1) конфиденциальности (несанкционированный доступ, несанкционированное использование, раскрытие), 2) целостности (несанкционированное изменение или уничтожение информации), 3) доступности (обеспечение своевременного и надежного доступа к информации авторизированным пользователям).[53]

В США в документах, касающихся информационной безопасности, наибольший акцент делается в защиту информации и поддерживающей инфраструктуры.

В Китайской Народной Республике (КНР) информатизацию называют обязательным условием модернизации производства, а сетевую безопасность – важным элементом национальной безопасности. КНР, в противопоставление США, предлагает концепцию киберсуверенитета – развития, использования и государственного регулирования сети Интернет внутри своих границ без возможности вмешательства других государств[54].

---

[52] Регламент (ЕС) относительно Агентства Европейского Союза по сетевой и информационной безопасности: № 526/2013 от 21.05.2013. [online]. *Официальный сайт Европейского Союза*, 2021 [citat 23.09.2021]. Доступен: https://eur-lex.europa.eu/eli/reg/2013/526/oj

[53] КАРАСЕВ, П. А. Стратегия информационной (кибер) безопасности США в XXI веке В: *Вестник Московского Университета. Серия 12: Политические науки*. 2013, № 2, с. 82-102. ISSN 0868-4871.

[54] МИХАЛЕВИЧ, Е. А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность В: *Вестник Российского университета дружбы народов. Серия: Политология*, 2021, 23(2), 254–264. ISSN 2313-1446.

В КНР под информационной безопасностью понимается «защита оборудования, программного обеспечения, данных и предоставляемых услуг информационной системы с целью обеспечения непрерывной и надежной работы от несанкционированного доступа, утечки, случайного или преднамеренного уничтожения или модификации, просмотра, проверки, записи или уничтожения. Основными составляющими информационной безопасности являются подлинность, конфиденциальность, целостность, безотказность, готовность, проверяемость и управляемость» [55].

В РФ были приняты две Доктрины информационной безопасности: 9 сентября 2000 года и 5 декабря 2016 года, Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". В Доктрине 2016 года понятие информационной безопасности формулируется как «*состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства*».

Анализ доктрин ведущих держав мира в области информационной безопасности позволяет увидеть различие в подходах. В США во главу угла ставится доступность и открытость интернет-пространства, отсутствие границ и цензуры. Для ЕС характерен наиболее жесткий подход к защите персональных данных своих граждан. В КНР введены наибольшие ограничения по обмену и распространению информации. В РФ и КНР для обеспечения информационной безопасности от внешних угроз декларируется необходимость киберсуверенитета государства в информационном пространстве.

Общим для всех Доктрин является понимание, что информационная безопасность является важным компонентом системы национальной безопасности. Наиболее подвержены угрозам оборонная, государственная и общественная, экономическая, научно-техническая и образовательная сферы. Источниками угроз называют внутреннюю и внешнюю среду, и они направленны в основном на нарушение целостности, конфиденциальности и доступности информации и поддерживающей инфраструктуры.

Понятие «информационная безопасность» в международных стандартах

Лучшие практики в обеспечении безопасности информационных систем отражены

[55] РОМАШКИНА, Н. ЗАДРЕМАЙЛОВА, В. Эволюция политики КНР в области информационной безопасности В: *Пути к миру и безопасности*. 2020, № 1(58), с. 122-138. ISSN 2307-1494.

в международных (ISO/IEC, ISF, CobIT и др.) и национальных стандартах (NIST – США, BS – Великобритания, ГОСТ – РФ, BSI – ФРГ и др.).

Наиболее популярным является международный стандарт ISO/IEC 27002:2013 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью" (Information technology. Security techniques. Code of practice for information security management)». В нем из постулата, что информация является ценным бизнес-ресурсом, следует вывод о необходимости применения политик, рекомендаций, инструкций, организационных структур и программных функций для обеспечения ее защиты от разнообразных угроз для поддержки бизнеса с помощью сохранения таких характеристик информации как целостность, конфиденциальность и доступность для авторизированных пользователей.

Заметно, что понятия «целостность», «конфиденциальность» и «доступность» встречаются как в законодательных и нормативных актах, так и в стандартах в области информационной безопасности.

Под *конфиденциальностью* в стандарте ISO/IEC 27002:2013 понимается предоставление доступа к информации, только имеющим на это право пользователям. *Целостность* информации подразумевает ее точность и полноту. Доступ к информационным ресурсам авторизированным пользователям по мере необходимости называется *доступностью*.

Понятие «информационная безопасность» в научной литературе

В научной литературе понятие «информационная безопасность» трактуется либо в соответствии с законодательными актами, либо согласно стандартам, либо с точки зрения отрасли знаний, в которой специализируется автор. Некоторые определения данного понятия представлены в Приложении 2.

Многие учебные пособия содержат определение информационной безопасности соответствующие Стандарту ISO / IEC 17799. Например, в учебнике Popa Sorin Eugen «Безопасность информационных систем» (2007) информационная безопасность определена как «*более широкое понятие, которое относится к обеспечению целостности, конфиденциальности и доступности информации*» [56, с. 5] .

В работе Mihai I.-C., Ciuchi C., Petrică G.-M., посвященной актуальным проблемам кибербезопасности, кибернетическая безопасность, также как и у Стрельцова А. А., связана, хотя и не считается идентичной, с концепцией информационной безопасности.

[56] POPA, S. E. *Securitatea sistemelor informatice. Note de curs şi aplicaţii pentru studenţii Facultăţii de Inginerie*. Bacău: Editura Alma Mater, 2007. 136 p. ISBN: 978-973-1833-21-7.

Последнюю авторы определяют как «*деятельность по защите информации и компьютерных систем от несанкционированного доступа, использования, раскрытия, прерывания, изменения или уничтожения для обеспечения целостности, конфиденциальности и доступности информации*»[57, с.23-24].

Загорский А. В., Ромашкина Н. П. относят защиту информации и каналов ее передачи к системе задач из области международной этики, права, организации управления, разработки технических средств, программирования и математики, – необходимых для обеспечения информационной безопасности личности, общества и государства. Выделяют две сферы информационной безопасности: информационно-техническую и информационно-психологическую, отвечающих принципам доступности, аутентичности, целостности и конфиденциальности. Особое внимание уделяют информационным методам воздействия и противоборства в международных конфликтах XXI века [58, с. 23].

С позиции системного подхода к вопросам информационной безопасности подходят и авторы многократно переиздаваемого учебного пособия для студентов высших учебных заведений «Информационная безопасность и защита информации» Московского Авиационного Института – Мельников В. П., Клейменов С. А. и Петраков А. М.. Комплексным обеспечением информационной безопасности авторы называют систему организационно-правовых, физических, социальных, духовных, информационных, программно-математических и технических методов, мероприятий и средств, необходимых для обеспечения нормального функционирования государства, населения, организаций и предприятий на собственной территории и в международном пространстве [59, с. 29].

Арсентьев М. В. рассматривает явление ИБ с позиции теории информационных процессов и систем. Информация, являясь идеальным объектом, обладает ценностью, то есть уменьшает неопределенность. При этом информация не может существовать без материального носителя. Пересечение информационных процессов, наличие информационного аспекта во всех видах человеческой деятельности приводит к неопределенности понятия информация, а далее и информационной безопасности. Говоря

---

[57] MIHAI, I.-C., CIUCHI, C., PETRICĂ, G.-M. *Provocări actuale în domeniul securității cibernetice - impact și contribuția României în domeniu.* București, 2018. 89 p. ISBN 978-606-8202-60-0.

[58] ЗАГОРСКИЙ, А. В., РОМАШКИНА, Н. П. *Угрозы информационной безопасности в кризисах и конфликтах XXI века.* Москва: ИМЭМО РАН, 2015. 151 с. ISBN 978-5-9535-0450-8.

[59] МЕЛЬНИКОВ, В. П., КЛЕЙМЕНОВ, С. А., ПЕТРАКОВ, А. М. *Информационная безопасность и защита информации.* 3-е изд. Москва: Издательский центр «Академия», 2008. 336 с. ISBN 978-5-7695-4884-0.

об информации как объекте защиты, ученый акцентирует особое внимание на субъекте информационных отношений. Субъекты информационной безопасности, обладая ценной информацией, имеют определенные преимущества в условиях конкуренции, противоборства, соперничества. Автор определяет степень информационной безопасности субъекта в зависимости от уровня доступа к информационной среде, осознания угроз, владения средствами их отражения, и подчеркивает, что субъективная оценка безопасности может отличаться от реальной ситуации в зависимости от уровня компетентности субъекта. Субъекты информационных отношений также могут представлять потенциальные или реальные угрозы информационной безопасности. Рассматривая явление ИБ с объективной и субъективной позиции, Арсентьев предлагает рассматривать информационную безопасность как уменьшение информационной неопределенности относительно существующих потенциальных и реальных угроз и наличия возможностей и инструментов их отражения [60].

Многие авторы замечают, что на уровне государства защита информации находится на высоком уровне: есть законодательные и нормативные акты, четко разработанные регламенты и стандарты. Гораздо больше проблем с информационной безопасностью возникает на уровне общества и личности. Некоторые труды именно этому и посвящены.

В книге Курило А. П., Зефирова С. П., Голованова В. Б. информационная безопасность рассматривается на уровне организации как «*состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере*»[61, с. 32].

Курило А. П. – один из создателей Стандарта Банка России по обеспечению информационной безопасности в банковской сфере, законодательства в области защиты информации, Доктрин информационной безопасности, – анализирует этот феномен с точки зрения системного и процессного подходов. Для обеспечения состояния защищенности информации в современном контексте ученый к целостности, конфиденциальности и доступности (ставшими уже классическими в определении информационной безопасности) добавляет свойства аутентичности, подотчетности, неотказуемости и надежности, необходимые [62, с. 30].

---

[60] АРСЕНТЬЕВ, М. В. К вопросу о понятии «информационная безопасность». В*: Информационное общество*. 1997, № 4-6. с. 48-50.

[61] КУРИЛО, А. П., ЗЕФИРОВ, С. П., ГОЛОВАНОВ, В. Б. *Аудит информационной безопасности*. Москва: Издательская группа «БДЦ-пресс», 2006. 304 с. ISBN 5-93306-100-X.

[62] КУРИЛО, А. П., МИЛОСЛАВСКАЯ, Н. Г., СЕНАТОРОВ, М. Ю., ТОЛСТОЙ, А. И. *Основы управления информационной безопасностью*. 2-е изд. Москва: Горячая линия-Телеком, 2014. 244 с. ISBN 978-5-9912-

В учебнике Корнеева И. К. и Степанова Е. А. информационная безопасность понимается как составная часть экономической безопасности предприятия наравне с физической, правовой и маркетинговой безопасностью. Направлениями информационной безопасности авторы называют аудит информации предприятия и определение ее ценности, актуализацию угроз, формирование комплексной системы защиты информации в электронном и традиционном документообороте в технических каналах и от персонала [63, с. 30].

Малюк А. А. в учебном пособии, предназначенном для студентов, обучающихся не по специальностям в области информационной безопасности, разделяет опасности для накапливаемой, хранимой и обрабатываемой в автоматизированной системе информации на два класса: во-первых, нарушение физической целостности (искажение или уничтожение), и, во-вторых, несанкционированный доступ неавторизированных лиц. Первую опасность автор связывает с развитием технологии автоматизированной обработки информации, а вторую с человеческим фактором, который приобретает все большее значение в инцидентах, относящихся к реализации угроз информационной безопасности [64, с. 3].

Платонов В. В. в учебнике по программно-аппаратным средствам защиты информации определяет информационную безопасность как защищенность информации и поддерживающей инфраструктуры от ущерба, естественного или искусственного характера нанесенного случайно и преднамеренно [65, с.13] .

В большинстве учебников по информационной безопасности рассматриваются программно-технические [Андрончик А. Н., Богданов В. В.; Емельянова Н. З., Партыка Т. П., Попов И. И.; Игнатьев В. А.; Каторин Ю. Ф., Разумовский А. В., Спивак А. И.; Платонов В. В.; Пролетарский А. В., Суворов А. М., Смирнова Е. В., Руденков Н. А.; Торокин А. А., Ярочкин В. И.] и математические [Романец; Малюк А. А., Пазизин С. В., Погожин Н. С.; Нестеров С. А.] способы обеспечения информационной безопасности. В комплексе вопросы информационной безопасности рассматриваются в работах Бакланова В. В.; Мельникова В. П., Клейменова С. А., Петракова А. М.; Шаньгина В. Ф.; Зима В. М., Молдовяна А. А.

0271-8.

[63] КОРНЕЕВ, И. К., СТЕПАНОВ, Е. А. *Защита информации в офисе*. Москва: ТК Велби, Изд-во Проспект, 2008. 336 с. ISBN 978-5-482-01976-4.

[64] МАЛЮК, А. А., ПАЗИН, С. В., ПОГОЖИН, Н. С. *Введение в защиту информации в автоматизированных системах*. Москва: Горячая линия-Телеком, 2001. 148 с. ISBN 5-93517-062-0.

[65] ПЛАТОНОВ, В. В. *Программно-аппаратные средства защиты информации*. Москва: Издательский центр «Академия», 2013. 336 с. ISBN 978-5-7695-9327-7.

Вопросам правовой и организационной защиты посвящены работы Поляковой Т. А., Стрельцова А. А., Пожарского В. Н., Минаева В. А., Тарапановой Е. А., Фролова Д. Б., Скрыль С. В., Сычева А. М., Коробец Б. Н., Вайц Е. В., Грачева Ю. В., Астрахова А. В. и др. В юридическом поле возникло понятие информационного права, направленного на регулирование информационного пространства, прав и свобод общества и гражданина. Все это в настоящее время проходит этап становления [66, с. 113].

Специалисты в области юриспруденции, Полякова Т. А., Стрельцов А. А., рассматривают информационную безопасность с позиции защищенности человека, общества и государства в информационной сфере, а также – как результат противодействия с помощью специальных средств угрозам безопасности в информационной сфере [67, с. 15].

Практически во всех определениях информационной безопасности упоминаются угрозы ее нарушения. К ним принято относить, ставшие классической триадой, основные категории, предложенные одним из пионеров[68] информационной безопасности James P. Anderson [69], описанные исследователями Массачусетского Технологического Университета Jerry Saltzer и Michael Schroeder в статье «Защита информации в компьютерных системах» (1975): 1) неавторизованное раскрытие информации; 2) неавторизованное изменение информации; 3) неавторизованный отказ в доступе.

Термин «неавторизованный» в трех перечисленных выше категориях означает, что раскрытие информации, ее модификация или отказ в доступе к ней происходит вопреки желанию владельца или законного пользователя информации, возможно даже в противодействие существующей системы защиты. Самой большой проблемой является то, что «злоумышленником» может оказаться законный пользователь компьютерной системы [70].

В современной литературе, правовых актах и стандартах применяются

---

[66] НИКОДИМОВ, И. Ю. Современные проблемы теории информационного права. В: *Вестник Московского государственного лингвистического университета. Образование и педагогические науки*». 2016, №2 (766), с. 105-117. ISSN 2500-3488

[67] ПОЛЯКОВА, Т. А., СТРЕЛЬЦОВ, А. А. *Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры*. Москва: Юрайт, 2016. 325 с. ISBN 978-5-9916-6799-9.

[68] SPAFFORD, E. James P. Anderson: An Information Security Pioneer. In: *IEEE Security and Privacy Magazine.* February 2008. 6 (1). p. 9 DOI:10.1109/MSP.2008.15

[69] ANDERSON, J. Information security in a multi-user computer environment. In: *Advances in Computers*, vol. 12. New York: Academic Press, 1973, pp. 1-35. (I A1, SFR) DOI: 10.1016/S0065-2458(08)60506-9

[70] SALTZER, J. H. SCHROEDER, M. D. The protection of information in computer systems. In *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278-1308, Sept. 1975, DOI: 10.1109/PROC.1975.9939 URL: web.mit.edu/Saltzer/www/publications/protection/index.html

определения: конфиденциальность (confidentiality), целостность (integrity) и доступность (availability) – эти три основные угрозы информационной безопасности носят название триада CIA [71]. Исходя из международных стандартов по информационной безопасности, нормативно-правовых актов и научной литературы, можно сформулировать угрозы следующим образом: 1) угроза нарушения конфиденциальности: несанкционированное разглашение информации; 2) угроза нарушения целостности: несанкционированное изменение или удаление информации; 3) угроза нарушения доступности: несанкционированный запрет авторизированному пользователю к информации в момент необходимости. Для сравнения изначального определения триады угроз информационной безопасности и современного понимания в стандартах в данной области автором составлена таблица, представленная в Приложении 3.

Нетрудно заметить, что в большинстве определений информационной безопасности встречается упоминание либо перечисление средств защиты. Существуют различные классификации средств защиты. Основываясь на анализе работ ученых и специалистов в области информационной безопасности, таких, как Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф., Герасименко В. А., Блинов А. М., Емельянова Н. З., Партыка Т. Л., Попов И. И. , Бондарев, В. В. , Курило А. П., Зефиров С. П., Голованов В. Б., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И., Малюк А. А., Пазин С. В., Погожин Н. С., Мельников В. П., Клейменов С. А., Петраков А. М., Ясенев В. Н., Дорожкин А. В., Сочков А. Л., Ясенев О. В., Ярочкин В. И., Поляков В. П. и др. можно сказать, что эффективная защита информации может быть достигнута только реализацией целого комплекса мер. К системе защиты будем относить следующие средства:

– законодательные – юридические нормы (законы, указы и другие нормативные акты), регламентирующие обращение с информацией ограниченного использования и ответственность за их нарушение;

– морально-этические – нормы поведения принятые в обществе, неприятие которых ведет к падению престижа человека их не соблюдающего;

– организационные – регламентация на уровне организации, призванная определить порядок взаимодействия сотрудников и информационной системы для уменьшения вероятности реализации угроз целостности, конфиденциальности и доступности;

– программно-технические – электронные устройства и программное обеспечение

[71] SMITH, R. E. *Elementary Information Security*. Burlington: Jones & Bartlett Learning, 2013. 892 p. ISBN 978-1-4496-4820-6.

(зачастую применяющие криптографические методы) для идентификации и аутентификации пользователей, разграничения уровней доступа, контроля целостности данных, регистрации событий в информационной системе и т.п.;

– физические – препятствия на пути проникновения к защищаемой информации в виде механических устройств, сооружений, систем сигнализации и видеонаблюдения и т. д..

На основе анализа рассмотренных определений информационной безопасности, представлена схема, в которой отражены, на наш взгляд, ориентиры необходимые для подготовки курса при изучении основ защиты информации будущими специалистами финансово-экономической сферы (рис. 1.2).

Анализируя нормативные акты различных государств, международные стандарты, научную литературу, пришли к выводу, что для нас наиболее близким будет определение информационной безопасности, которое будет отражать основные угрозы, средства защиты информационных ресурсов для личности, общества и государства.

Немного перефразируя Полякову Т. А. и Стрельцова, определим информационную безопасность как «*результат противодействия угрозам безопасности человека, общества и государства в информационной сфере, осуществляемого с использованием выделенных для этого сил и средств*».

Овладение всем спектром средств защиты информации представляет собой интеграцию знаний, умений и навыков из разных областей знаний: юриспруденция, инженерные науки, математика, психология, информационные технологии, история, этика и так далее.

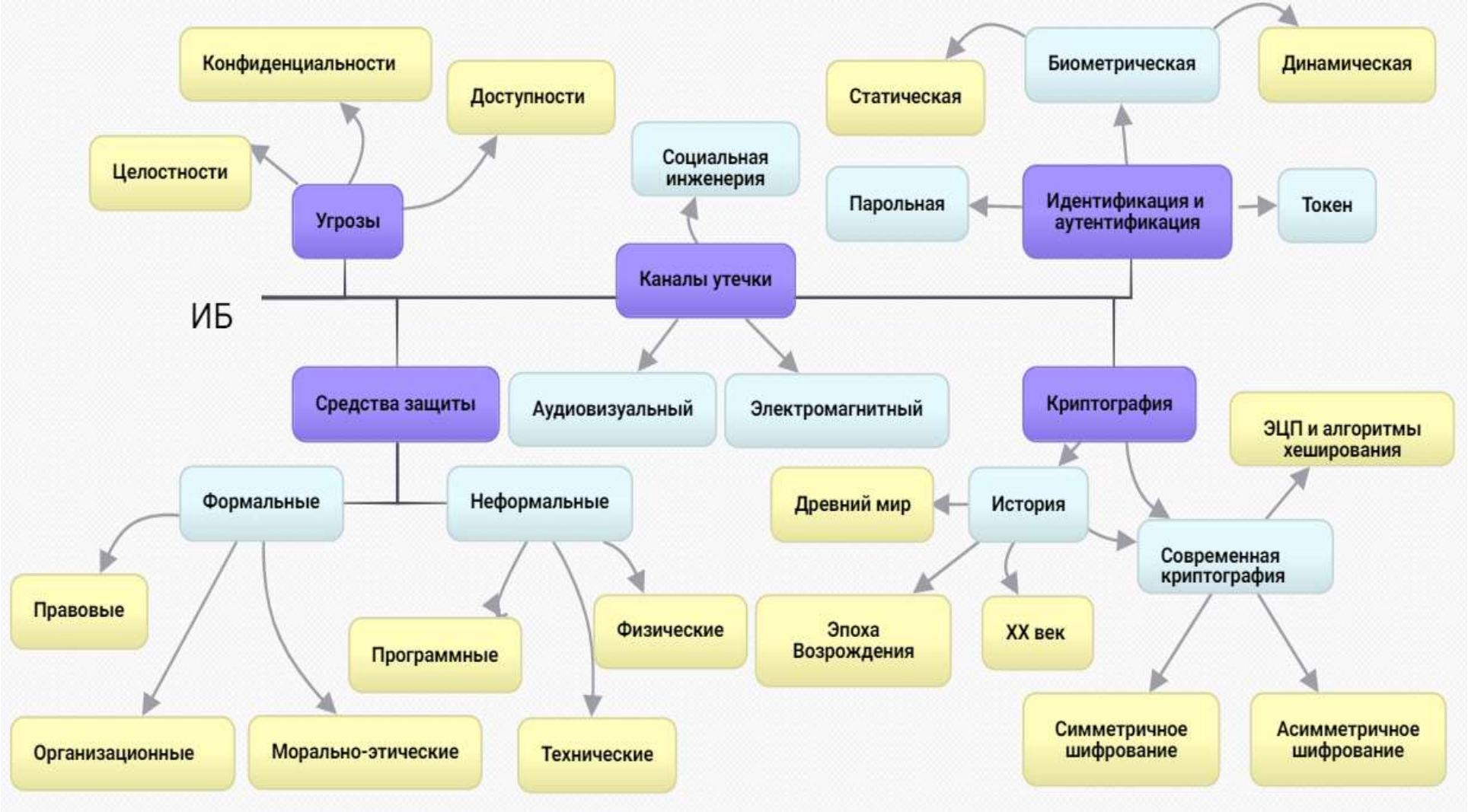


Рис. 1.2. Направления изучения в рамках дисциплины ИБ

* разработано автором средствами он-лайн сервиса bubbl.us

1.2 Информационная безопасность как элемент цифровой грамотности

Активное применение информационных технологий во всех сферах экономики свидетельствует о высоком спросе на обладание цифровыми навыками потенциальных работников. Набор цифровых навыков формирует цифровую грамотность. К ключевым навыкам цифровой грамотности Институт ЮНЕСКО по информационным технологиям и образованию относит компьютерную грамотность, связь и сотрудничество, создание цифрового контента, безопасность, решение проблем и компетенции, связанные с карьерой. В области «безопасность» определены конкретные компетенции: умение применять защитные устройства, защищать персональные данные и соблюдать правила конфиденциальности, защищать здоровье, защищать окружающую среду[72]. Эти компетенции перекликаются с навыками, сформулированными в европейской рамке квалификаций.

Категории *компетенция* и *компетентность* неоднозначные, так как существует множество определений. Согласимся с определением Хуторского А. В., что компетентность как владение компетенцией. В диссертационном исследовании часто будет встречаться термин цифровая компетентность.

В Стандарте цифровых компетенций, сформулированная, для дидактических работников общего образования в РМ (Standarde de competențe digitale pentru cadrele didactice din învățământul general, Chişinău 2015) цифровая компетенция определена как «*интеграция знаний, навыков, умений, установок и ценностей, формируемых и развиваемых в процессе обучения, которыми обладает личность и которые могут быть мобилизованы для решения различных задач, возникающих в процессе сбора, хранения, обработки и распространения информации, с помощью информационных и коммуникационных технологий*». В области цифровых навыков «Соблюдение этических и правовых норм в цифровом пространстве» говорится о том, что пользователь на базовом уровне «*использует предустановленные инструменты кибербезопасности для защиты персональных данных и оборудования в личной цифровой среде (антивирус, брандмауэр, пароли)»,* на среднем уровне – «*выбирает стратегии безопасности в зависимости (антивирус, брандмауэр, пароли); выявляет угрозы безопасности и обращается за помощью для их устранения*», на продвинутом уровне – «*настраивает приложения кибербезопасности в соответствии с требованиями по устранению неполадок;*

---

[72] *Институт ЮНЕСКО по информационным технологиям в образовании*. ИИТО ЮНЕСКО © 1997-2022 [citat 23.10.2021]. Доступен: https://iite.unesco.org/ru/

устраняет угрозы безопасности, с которыми он сталкивается».

Европейская рамка квалификаций разработана с целью повышения прозрачности квалификации и мобильности граждан в Европе (включая Европейский Союз, Европейскую экономическую зону и страны-кандидаты в ЕС) Главным управлением образования и культуры Европейского Союза. В цифровую компетенцию входят навыки: 1) обработка информации; 2) коммуникация; 3) создание контента; 4) безопасность; 5) решение проблем. В сетке самооценки цифровых компетенций согласно Europass в части информационной безопасности представлены три вида пользователей: обычный, независимый и продвинутый (табл. 1.2).

Таблица 1.2. Сетка самооценки компетенции «Безопасность»[73]

Обычный пользователь	Независимый пользователь	Продвинутый пользователь
Я могу предпринять основные шаги для защиты своих устройств (например, с помощью антивирусов и паролей). Я знаю, что не вся информация в Интернете надежна. Мне известно, что мои учетные данные (имя пользователя и пароль) могут быть украдены. Я знаю, что я не должен раскрывать личную информацию в Интернете. Я знаю, что чрезмерное использование цифровых технологий может повлиять на мое здоровье. Принимаю элементарные меры по экономии энергии.	Я установил программы безопасности на устройства, используемые для доступа в Интернет (например, антивирус, брандмауэр). Я регулярно запускаю эти программы и регулярно их обновляю. Я использую разные пароли для доступа к оборудованию, устройствам и цифровым сервисам и периодически меняю их. Я могу идентифицировать веб-сайты или сообщения электронной почты, которые могут быть использованы для мошенничества. Я могу определить фишинговое письмо. Я могу формировать свою цифровую личность в Интернете и отслеживать свой цифровой след. Я понимаю риски для здоровья, связанные с использованием цифровых технологий (например, эргономика, риск зависимости). Я понимаю положительное и отрицательное влияние технологий на окружающую среду	Я часто проверяю конфигурацию безопасности и системы своих устройств и / или приложений, которые использую. Я знаю, как реагировать, если мой компьютер заражен вирусом. Я могу настроить или изменить настройки брандмауэра и безопасности своих цифровых устройств. Я знаю, как зашифровать электронную почту или файлы. Я могу применять фильтры к спам-сообщениям. Чтобы избежать проблем со здоровьем (физического и психологического), я разумно использую информационные и коммуникационные технологии. У меня есть осознанная позиция о влиянии цифровых технологий на повседневную жизнь, онлайн-потребление и окружающую среду.

По результатам опроса, проводимого среди студентов экономических специальностей перед изучением дисциплины «Информационная безопасность», более

[73] Europass: Digital competences – Self-assessment grid [online]. *Онлайн инструмент ЕС унифицированного сравнения квалификаций* , 2021 [citat 01.07.2021]. Доступен: europass.cedefop.europa.eu/sites/default/files/dc-en.pdf]

90% респондентов можно отнести к категории «Обычный пользователь» и менее 10% отвечают утвердительно на половину вопросов из категории «Независимый пользователь».

Региональным общественным центром интернет технологий (РОЦИТ) разработан индекс цифровой грамотности, состоящий из трех групп: цифровое потребление, цифровые компетенции и цифровая безопасность. Всего предложено 20 индикаторов. В группу «цифровая безопасность» входят навыки защиты персональных данных, обеспечения целостности информации, борьбы с компьютерными вирусами, негативное отношение к пиратскому программному обеспечению и пиратскому медийному контенту, высокий уровень культуры взаимодействия в социальных сетях и соблюдение этических норм при размещении цифрового контента[74].

В Республике Молдова в Национальной стратегии создания информационного общества «Электронная Молдова» говорится, что «*информационное общество является новой, более совершенной формой человеческой цивилизации, в которой равноправный и универсальный доступ к информации, связанный с развитием информационно-коммуникационной инфраструктуры, способствует стабильному социально-экономическому развитию, снижению уровня бедности, повышению качества жизни*» [75].

Таким образом, видим, что цифровая грамотность имеет большое значение для повышения качества жизни, доступности образования, и обучения на протяжении всей жизни. Работники, имеющие дело в своей профессиональной деятельности с потенциально ценной информацией, должны обладать навыками защиты информации от нарушения конфиденциальности, целостности и доступности.

1.3 Исследование стандартов и учебных планов подготовки экономических кадров в области информационной безопасности

Обзор стандартов и учебных планов подготовки экономических кадров в РМ

Фундаментальными нормативными документами при организации учебного процесса в вузе являются: образовательные стандарты, номенклатура специальностей, учебные планы и программы. В советское время эти документы разрабатывались централизовано на всесоюзном уровне, а после обретения независимости Республикой

[74] *Официальный сайт РОЦИТ*. ИИТО ЮНЕСКО © 1996-2022 [citat 01.02.2021]. Доступен: цифроваяграмотность.рф

[75] Постановление Правительства Республики Молдова о Национальной стратегии создания информационного общества - "Электронная Молдова": №255 от 09.03.2005. В: *Monitorul Oficial al Republicii Moldova*, 2005, nr. 46-50, 336.

Молдова разработка и адаптация образовательных стандартов к требованиям рынка труда стали обязанностью самих учебных заведений. Образовательные стандарты в Республике Молдова до 1998 года разрабатывались в виде квалификационных характеристик будущего специалиста, замененных в 2000 году на титульные характеристики. В период с 2002-2003 гг. разрабатывали Стандарты по различным направлениям профессиональной подготовки, определяющие общие и специфичные компетенции, требования к минимальному объему учебных программ.

Благодаря присоединению к Болонскому процессу в Республике Молдова применяется Национальная рамка квалификаций (НРК), соответствующая Европейской рамке квалификаций (EQF). НРК впервые опубликована в 2013 году, в 2017 году Правительство Республики Молдова утвердило новую НРК Постановлением №1016[76].

О необходимости обучения основам информационной безопасности будущих экономистов можно судить по Национальной рамке квалификаций Республики Молдова для экономистов уровня лицензиат. Правильная и быстрая передача информации является частью специфической компетенции «управление информацией» согласно Национальной рамке квалификаций Республики Молдова по направлению «Экономика». Обеспечение быстрой и правильной передачи информации тесно связано с информационной безопасностью (табл. 1.3).

Таблица 1.3. ИТ-компетенции будущих экономистов в НРК РМ

Рейтинг по важности	**Краткое наименование конкретных компетенций**	**Описание компетенций** *По завершении студент должен уметь*	**Уровень дескрипторов в Дублине**
1	базовые знания	1.6. Информационные системы - разработка и эксплуатация информационных систем и их влияние на деятельность 1.7. Информационные и коммуникационные технологии - знание и использование информационных и коммуникационных технологий в бизнесе	A, C A, C
2	управление информацией	14. Получать и эффективно использовать информацию в письменной, устной и невербальной форме, на родном и иностранном языках. 15. Применять эффективные количественные и качественные методы анализа информации. 16. Обеспечить быструю и правильную передачу информации.	D B, C D

[76] Постановление Правительства Республики Молдова об утверждении Национальной рамки квалификаций Республики Молдова: nr. 1016 от 23.11.2017. В: *Monitorul Oficial al Republicii Moldova*, 2017, nr. 421-427, 1137.

Вузами Республики Молдова в соответствии с НРК разработаны учебные планы для экономических направлений подготовки, в каждой из которых представлены различные дисциплины информационного цикла (табл. 1.4).

Таблица 1.4. Сравнительная характеристика информационных дисциплин в подготовке будущих экономистов в Республике Молдова

ВУЗ	Учебный план, направление и год подготовки	Курс, семестр, информационная дисциплина
Universitatea de stat din Moldova, Facultatea stiinte economice[77]	041 Ştiinţe economice 2017	Информационно-коммуникационные технологии (4 кредита, 120 часов: 60 ауд. и 60 сам.раб.)
Academia de studii economice din Moldova[78]	36. Științe economice 2016	Экономическая информатика (5 кредитов, 150 часов: 60 ауд. и 90 сам.раб.)
UTM	Economia Comerţului, Turismului şi Serviciilor 2019	Информационные технологии в бизнесе (1 курс, 1 семестр) Инструменты программного обеспечения в бизнесе (1 курс, 2 семестр)
Universitatea de Stat «Grigore Țamblac» din Taraclia[79]	041 Științe economice 2017	Экономическая информатика и вычислительная техника (1 курс, 1 семестр: 6 кредитов, 180 часов: 90 аудиторная,90 сам.раб.) Информационные технологии в бухгалтерском учете (3 курс, 5 семестр: 4 кредита, 120 часов: 60 ауд. и 60 сам.раб.)
Universitatea de Studii Europene din Moldova[80]	041 Științe economice 2017	Экономическая информатика (1 курс, 1 семестр: 5 кредитов, 150 часов: 60 ауд. и 90 сам.раб.) Информационные технологии в бизнесе (3 курс 5 семестр: 5 кредитов, 150 часов: 60 ауд. и 90 сам.раб.)
Institutul de relaţii internaţionale din Moldova [81]	0410. Economie 2019	Экономическая информатика (1 курс, 1 семестр: 3 кредита, 90 часов: 45 ауд. и 45 сам.раб.)

В дисциплину «Экономическая информатика» («Informatică economică») в Республике Молдова в соответствии с *Cadrul Naţional Al Calificărilor Învăţământ Superior Domeniul de formare profesională* входит изучение (Word, Excel, Acces). При этом по

[77] Plan de învăţământ. Ştiinţe economice [online]. *Caŭm Universitatea de Stat din Moldova,* 2021 [citat 01.02.2021]. Доступен: http://usm.md/wp-content/uploads/Marketing-si-logistica.pdf

[78] Plan de învăţământ. Ştiinţe economice. [online]. *Caŭm Academia de Studii Economice a Moldove*, 2021 [citat 01.02.2021]. Доступен: https://ase.md/files/planuri/2018/zi/EG.pdf

[79] 23. Plan de învăţământ. Ştiinţe [online]. *Caŭm Universitatea de Stat „Grigore Țamblac" din Taraclia*, 2020 [citat 02.06.2020]. Доступен: https://tdu-tar.md/images/files/3_uchebnyy_process/5_knigi_specialjnsotey/Manualul_specialit_Uch.pdf

[80] Plan de învăţământ. Ştiinţe economice. [online]. *Caŭm Universitatea de Studii Europene din Moldova*, 2021 [citat 01.02.2021]. Доступен: https://www.usem.md/uploads/files/Facultatea_Stiinte_Economice/Planuri_de_invatamint/Ciclul_I/2017/Planuri/0413_1%20Business%20și%20administrare.PDF

[81] Plan de învăţământ. Ştiinţe economice. [online]. *Caŭm Institutul de Relații Internaționale din Moldova*,2021 [citat 01.02.2021]. Доступен: http://irim.md/wp-content/uploads/2016/05/Plan-de-invatamint-Economie-Mondiala-si-Relatii-Economice-Internationale-Ciclul-I.pdf

профилю 364 «Finanţe» среди компетенций, связанных с информационными технологиями, можно выделить только одну: С11 «Умение оперировать информационными технологиями» (Capacitatea de operare cu tehnologii informaţionale*)*.По профилю 366 «Economie Generală» среди компетенций, связанных с информационными технологиями можно выделить также только одну: С8 – «Умение оперировать информационными технологиями» (Capacitatea de operare cu tehnologii informaţionale).

Как видим, отдельной компетенции в области информационной безопасности в НРК РМ не прописано.

Для примера в Украине в Стандарте по специальности 051 «Экономика» (уровня бакалавриат), утвержденном приказом №1244 Министерства образования и науки Украины от 13.11.2018 г. к общим компетенциям, касающихся информационных технологий, относят ЗК7 «Навыки использования информационных и коммуникационных технологий» и ЗК8 «Способность к поиску, обработке и анализу информации из различных источников», а к профессиональным: СК7 «Способность применять компьютерные технологии и программное обеспечение по обработке данных для решения экономических задач, анализа информации и подготовки аналитических отчетов» и СК10 «Способность использовать современные источники экономической, социальной, управленческой, учетной информации для составления служебных документов и аналитических отчетов». Каждый вуз сам разрабатывает свои учебные планы для достижения запланированных результатов,

В России Федеральный Государственный Образовательный Стандарт Высшего Образования 2015 года предписывает, что выпускник, освоивший программу бакалавриата по направлению подготовки 38.03.01 Экономика, должен обладать общепрофессиональной компетенцией ОПК-1 «*способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*». Таким образом, в Российской Федерации при подготовке экономических кадров явным образом учитывается аспект информационной безопасности при обучении информационным технологиям в профессиональной деятельности.

В зависимости от сферы деятельности делаются разные акценты в профессиональной подготовке специалистов при изучении дисциплин информационного цикла, а также информационной безопасности. Для юридических специальностей важно изучение правовых аспектов защиты информации, знание физических и технических

способов защиты. Для будущих медицинских работников важно понимание особенностей работы с персональными данными, программных и технических средств защиты от угрозы нарушения конфиденциальности, юридической ответственности за разглашение врачебной тайны в рамках развития электронной медицины. Будущие специалисты финансово-экономической сферы должны овладеть широким спектром средств защиты ценной информации, составляющей коммерческую тайну.

Приведем данные по изучению информационной безопасности будущими специалистами в области финансово-экономической сферы (табл. 1.5).

Таблица 1.5. Обзор обучения основ информационной безопасности будущими экономистами в вузах разных государств

Страна	ВУЗ	Направление и курс	Курс, семестр, информационная дисциплина и темы
Австралия	Monash Business School[82]	бакалавр информационных технологий, 1 курс, 2016 год набора	Дисциплина «Введение в компьютерные системы, сети и безопасность»
Россия	Высшая школа экономики, Пермь[83]	Дополнительный профиль для любой специальности, 3 курс бакалавры	Дисциплина «Информационная и экономическая безопасность». Знакомит с основами шифрования, способами защиты информации и информационных прав, мерами юридической ответственности за совершение экономических преступлений и правонарушений в информационной сфере
Румыния	“Alexandru Ioan Cuza” din Iaşi Факультет экономики и делового администрирования	лицензиат «Экономическая информатика», 3 курс, 2021	Дисциплина «Безопасность информационных систем»
		лицензиат «Бухгалтерские и управленческие информационные системы», 2 курс, 2021	Дисциплина «Защита и безопасность информационных систем»
США	Принстонский университет Институт компьютерных наук	Читается по выбору для любой специальности, 2 часа в неделю в течение 1 семестра, 2021	Дисциплина «Информационная безопасность» Темы: Как защитить вычислительные системы, коммуникации и пользователей. Базовая криптография. Приватное и аутентифицированное общение. Безопасность программного обеспечения. Вредоносное ПО. Защита

[82] Учебный план для бакалавров информационных технологий 2016 год. *Сайт Monash University in Melbourne Australia*. 2022 [citat 23.12.2020]. Доступен: https://www.monash.edu/business

[83] Элективный курс «Информационная и экономическая безопасность» [online]. *Сайт Национальный исследовательский университет «Высшая школа экономики»,* 2022 [citat 12.01.2022]. Доступен: https://electives.hse.ru/minor_security_perm/

			операционной системы. Сетевая безопасность. Веб-безопасность. Физическая защита. Криптовалюты и блокчейн. Конфиденциальность и анонимность. Полезная безопасность. Экономика безопасности. Этика безопасности. Правовые и политические вопросы [84]
Украина	Львовский Национальный Университет имени Івана Франка	направление подготовки бакалавров 6.030502 «Экономическая кибернетика» области знаний 0305 «Экономика и предпринимательство»	Дисциплина «Защита информации в информационных системах». Темы: «Общие аспекты защиты информации», «Криптографические методы защиты информации», «Безопасность в информационных сетях», «Правила безопасности в Internet», «Программные вирусы и способы их нейтрализации».
Украина	Харьковский Политехнический Институт		Дисциплина «Информационные системы» присутствует раздел «Информационная безопасность электронных информационных систем», в котором рассматриваются способы и средства защиты информации, идентификация и аутентификация пользователей, шифрование и обеспечение целостности данных.

Анализ учебных планов вузов различных стран говорит о том, что во всем мире наблюдается тенденция введения если не дисциплины «Информационная безопасность», то хотя бы отдельных тем при изучении курсов информационного цикла, либо как вариативный курс по выбору для любой специальности. Это согласуется с Доктринами информационной безопасности государств, в большинстве из которых говорится, что информационная безопасность является составляющей частью национальной безопасности государства и повышения информированности граждан и их грамотности в области информационной безопасности является приоритетом построения информационного общества.

1.4 Анализ профессиональной подготовки в области информационной безопасности

Трансформирование традиционной экономики в цифровую, из-за непрерывного бурного развития технологий, увеличивает разрыв между получаемыми в образовательных учреждениях знаниями, умениями и навыками в области

[84] Описание курса «Информационная безопасность». *Сайт Департамента компьютерных наук Принстонского университета США*, 2022. [citat 23.12.2021]. Доступен: https://www.cs.princeton.edu/courses/archive/fall21/cos432/

информационных технологий, и высоким уровнем требований рынка труда к информационной компетентности, в том числе и в области информационной безопасности. Это несоответствие происходит в большинстве сфер экономики. Решением проблемы видится многим международным организациям и аналитикам в переходе к новой образовательной парадигме – обучение в течение всей жизни (англ. lifelong learning) [85 , с. 35]. Обучение навыкам информационной безопасности должно начинаться со школьной скамьи, продолжаться в рамках профессионального образования, и дополнительного образования в течение всей жизни.

В рамках профессионального образования специалистов в области информационной безопасности готовят по направлениям: «Криптография», «Компьютерная безопасность», «Организация и технология защиты информации», «Комплексная защита объектов информатизации», «Комплексное обеспечение информационной безопасности автоматизированных систем», «Информационная безопасность телекоммуникационных систем», «Противодействие техническим разведкам» и т. п. Получаемая квалификация при этом «Математик» или «Специалист по защите информации».

Современные тенденции информатизации формируют потребность не только в высококвалифицированных кадрах в области информационной безопасности, но также выдвигают новые требования к специалистам из финансово-кредитной сферы, государственного управления, и других отраслей экономики. На уровне государства несанкционированное воздействие на информационно-коммуникационную сферу может привести к реализации территориальных, военных, террористических угроз. На уровне организации – к снижению эффективности деятельности, потери доли рынка, ослаблении конкурентных позиций и тому подобное. Таким образом, необходимость в овладении информационно-коммуникационными компетенциями в области информационной безопасности наблюдается при подготовке специалистов гуманитарного, экономического, юридического профилей, – тех, кто в своей профессиональной деятельности имеет непосредственный доступ к информации, требующей защиты.

При подготовке бакалавров по направлению подготовки 38.03.01 «Экономика» в федеральном государственном образовательном стандарте РФ (ФГОС РФ) от 30 ноября 2015 года сформулирована общепрофессиональная компетенция ОПК-1 «*способность решать стандартные задачи профессиональной деятельности на основе*

[85] АЙЗИКОВА, Л. В. К вопросу об обучении на протяжении жизни В: *Наука о человеке: гуманитарные исследования*. 2012, №1 (9), с. 35-41.

информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности». В ФГОС РФ от 12 августа 2020 года по направлению подготовки бакалавров 38.03.01 «Экономика» сформулированы новые универсальные и общепрофессиональные компетенции, в том числе ОПК-5 «*способность использовать современные информационные технологии и программные средства при решении профессиональных задач*»[86]. В новом ФГОС рекомендуется Организации образования определять профессиональные компетенции самостоятельно либо руководствуясь соответствующими профессиональными стандартами. Таким образом, лица, зачисленные на обучение в 2021 году по программе бакалавриата по направлению 38.03.01 «Экономика», обучаются по новому ФГОС РФ.

В образовательном стандарте указано, что в процессе обучения должно быть предусмотрено широкое использование активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью активизации учебной деятельности студентов и формирования у них необходимых профессиональных компетенций. Однако, в образовательном стандарте не содержится явных указаний, как и какими средствами интерактивность может быть обеспечена. Это решение принимает преподаватель. Более детально активные и интерактивные методы обучения технологиям защиты информации будущих специалистов финансово-экономической сферы рассмотрены в Главе 2.

Большинство методических разработок по защите компьютерной информации предназначены для технических специальностей. В них рассматриваются технические, программные средства защиты информации. Особое внимание уделяется вопросам криптографической защиты.

Преподавание дисциплины «Информационная безопасность» для нетехнических специальностей, таких как «Экономика», «Менеджмент» осложняется недостатком соответствующей методической литературы. Методические рекомендации для гуманитарных специальностей чаще всего содержат материалы по защите информации в офисных программах и документов.

В Принстонском университете Институт компьютерных наук в описании курса «Информационная безопасность», читаемом для любой специальности, говорится, что «в

---

[86] Приказ Минобрнауки РФ от 12.08.2020 N 954 "Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 38.03.01 Экономика" (Зарегистрировано в Минюсте РФ 25.08.2020 N 59425) [online]. *Сайт Минюсте РФ,* 2021. [citat 23.10.2021]. Доступен: https://minjust.consultant.ru/documents/46969?items=1&page=1

этом курсе нет обязательных или рекомендуемых учебников, потому что нет ни одной книги, которая бы освещала правильный материал в актуальном состоянии». Слушателям предлагают темы: 1) Как защитить вычислительные системы, коммуникации и пользователей. 2) Базовая криптография 3) Приватное и аутентифицированное общение. 4) Безопасность программного обеспечения. 5) Вредоносное ПО. 6) Защита операционной системы. 7) Сетевая безопасность. 8) Веб-безопасность. 9) Физическая защита. 10) Криптовалюты и блокчейн. 11) Конфиденциальность и анонимность. 12) Полезная безопасность. 13) Экономика безопасности. 14) Этика безопасности. 15) Правовые и политические вопросы[87].

Особенности подготовки будущих экономистов в области информационной безопасности представлены в диссертационных исследованиях Полякова В. П. (2006)[88], Абиссовой М. А. (2006)[89], Горбунова А. И.(2011) [90].

В нашей работе рассматривается подготовка будущих экономистов в области информационной безопасности. В своей профессиональной деятельности выпускники экономических специальностей имеют дело с потенциально ценной информацией. В цифровой экономике растут объемы обрабатываемой информации, и вопросы безопасной работы с информацией становятся особенно острыми, т.к. количество угроз постоянно увеличивается. Студенты экономического профиля подготовки должны владеть в первую очередь организационно-управленческими способами защиты информации, быть осведомленными обо всех современных тенденциях и направлениях защиты информации.

Специфика преподавания дисциплины «Информационная безопасность» для будущих экономистов состоит в том, что обычно студенты по этим направлениям обладают разным уровнем знаний, умений и навыков в области информационных технологий. О противоречиях между востребованностью навыков в области информационной безопасности у нетехнических специалистах и уровнем их подготовки говорится в диссертационных работах российских ученых Абиссовой М. А., Боярова Е. Н., Ломаско, Полякова В. П., Тановой Э. В., Горбунова А. И.

---

[87] Описание курса «Информационная безопасность» Института компьютерных наук Принстонского Университета США. [citat 23.12.2021]. Доступен: https://www.cs.princeton.edu/courses/archive/fall21/cos432/

[88] ПОЛЯКОВ, В. П. О системе обучения студентов основам информационной безопасности. В: *Вестник ФА.* 2006, № 3 (39), с. 125-136.

[89] АБИССОВА, М. А., ФОКИН, Р. Р. Сервисы обучения информационной безопасности в курсе информатики для студентов гуманитарных и социально-экономических специальностей. В: *Педагогическая информатика. Специальный вып*уск. 2006, № 6, с. 115–117.

[90] ГОРБУНОВ А. И. Сущность и содержание профессиональной компетентности экономистов в области информационной безопасности. В: *Мир науки, культуры, образования*. 2011, № 6 (31), с. 155-158. ISSN 1991-5497.

Методология обучения технологиям защиты информации по различным специальностям в рамках вузовской подготовки представлены в диссертационных работах ученых:

– Алтуфьевой А. А. – обучение информационной безопасности специалистов безопасности жизнедеятельности (2008 год) [91];

– Боярова Е. Н. – разработка концептуальных подходов к обучению будущих специалистов в области информационной безопасности (2008 год)[92];

– Ломаско П. С. – подготовка в области информационной безопасности будущих учителей информатики (2009 год) [93];

– Матвеева Н.А. – развитие компетентности в области информационно-психологической безопасности в вузах МЧС России (2011 год)[94];

– Димова Е. Д. – обучение технологиям защиты информации специалистов в области прикладной информатики (2013 год) [95] и др.

В работах Тановой Э. В.[96], Синицына Д. С.[97], Малых Т. А.[98], Серебряника Е. Э.[99] предложены методы развития компетенций в области защиты информации у школьников.

Работы Полякова В. П., Абиссовой М. А. посвящены проблемам развития компетенций в области информационной безопасности в вузе у студентов, обучающихся по гуманитарным и социально-экономическим специальностям.

Поляков В.П. предложил не только ввести обязательную учебную дисциплину «Информационная безопасность», но и уделять внимание вопросам защиты информации в рамках всех учебных дисциплин, связанных с информационными технологиями, на всех уровнях подготовки: от школьного до послевузовского образования. В своей

---

[91] АЛТУФЬЕВА, А. А. *Методические основы обучения информационной безопасности на базе телекоммуникационных ресурсов сети Интернет:* автореф. дис. канд. пед. наук. Санкт-Петербург, 2008. 20 с.

[92] БОЯРОВ, Е. Н. *Концептуальные подходы к обучению специалиста информационной безопасности в университете*: дис. канд. пед. наук. Санкт-Петербург, 2008. 151 с.

[93] ЛОМАСКО, П. С. *Методическая система подготовки учителя информатики в области информационной безопасности:* автореф. дис. . канд. пед. наук. Красноярск, 2009. 25 с.

[94] МАТВЕЕВ, Н.А. *Педагогическая модель развития компетентности в области информационно - психологической безопасности у курсантов вузов ГПС МЧС* России: автореф. дис. канд. пед. наук. Санкт-Петербург, 2011. 22 с.

[95] ДИМОВ, Е. Д. *Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования*, дис.канд. пед. наук. Москва, 2013.181с.

[96] ТАНОВА, Э. В. *Формирование компетентности в области защиты информации у школьников в процессе обучения информатике:* автореф. дис. канд. пед. наук. Екатеринбург, 2005, 2012. 23 с.

[97] СИНИЦЫН, Д.С. *Психолого–педагогические условия обучения информационно-психологической безопасности подростков*: дис. канд. пед. наук. Санкт-Петербург, 2005. 169 с.

[98] МАЛЫХ, Т.А. *Педагогические условия развития информационной безопасности младшего школьника:* дис.канд. пед. наук. Иркутск, 2008. 168 с.

[99] СЕРЕБРЯНИК, Е.Э. *Формирование информационно–личностной безопасности учащихся основной школы:* дис. канд. пед. наук. Калининград, 2011. 183 с.

диссертационной работе Поляков В. П. пишет, что «несмотря на важность, актуальность и значимость обеспечения информационной безопасности сама теория информационной безопасности находится в состоянии становления и далека от аксиоматики» [100, с.27]. Ученый описал методическую систему обучения информационной безопасности как «сложную открытую динамическую систему, которая должна охватывать все уровни, виды и направления высшего образования. Её содержательное наполнение … должно предусматривать, помимо специальных дисциплин по основам информационной безопасности, дисперсное включение отдельных вопросов обеспечения информационной безопасности в соответствующие темы информатики, информационных и коммуникационных технологий (безопасность операционных систем, безопасность в базах данных, безопасность офисных приложений, безопасность при работе в сети и т.п.)» [101].

В диссертационном исследовании Абиссовой М. А. рассмотрены сервисы обучения информационной безопасности студентов гуманитарной и социально-экономической направленности. Автор, проанализировав содержание преподаваемой на различных специальностях дисциплины «Информационная безопасность», акцентирует внимание на том, что содержание не отражает многих важных аспектов, таких как управление рисками, инженерно-технической защиты информации, криптоанализа и т. п. Марина Алексеевна подчеркивает, что дисциплина «Информационная безопасность» необходима не только будущим бакалаврам и магистрам в области информационных технологий, но и для физико-математического образования, естественно-научного, социально-экономического, филологического, юридического и других областей[102, с. 35].

Таким образом, обучение основам информационной безопасности важно и необходимо, но существующие методики необходимо адаптировать под современные стандарты и требования рынка труда, т.к. происходят постоянные изменения в информационной отрасли, знания и навыки быстро теряют свою актуальность.

---

[100] ПОЛЯКОВ, В. П. *Методическая система обучения информационной безопасности студентов вузов*: дис. ... д-ра пед. наук. Н. Новгород, 2006. 538 с.
[101] там же
[102] АБИССОВА, М. А. *Сервисы обучения информационной безопасности в теории и методике обучения информатике студентов гуманитарных и социально-экономических специальностей*: дис. . канд. пед. наук. Санкт-Петербург, 2006. 214 с.

1.5 Выводы к главе 1

В первой главе «Психолого-педагогические основы обучения информационной безопасности студентов экономических специальностей» рассмотрены феномены информационная безопасность как область знаний, изучены навыки из области информационной безопасности как составной части цифровой грамотности, проанализирована подготовка специалистов в области информационной безопасности, исследованы стандарты подготовки будущих экономистов в области информационной безопасности.

1. Показано, что организация обучения основам информационной безопасности будущих экономистов имеет свои особенности, связанные с сложностью и неоднозначностью понятийного аппарата, недостаточной разработанности методологических подходов к обучению основам информационной безопасности студентов нетехнических специальностей, разнообразием содержательной части в различных учебно-методических материалах.

2. Выявлено, что понятие «информационная безопасность» достаточно сложное, требующее системного подхода. Информационную безопасность можно рассматривать с различных уровней: личности, общества, государства. А также с различных научных точек зрения: с правовой, психологической, инженерно-технической, физической, организационной.

3. Внедрение информационных технологий, в том числе интернет-технологий, в процесс изучения вузовской дисциплины «Информационная безопасность» согласно результатам национальных и международных исследований вносит значительный вклад в повышение академической успеваемости и повышение личной заинтересованности и мотивации студентов, способствуя процессу интеграции будущих специалистов экономико-финансовой сферы на рынке труда.

4. Уникальный опыт, традиции и лучшие практики, накопленные в международной и отечественной системе высшего образования, по обучению специалистов финансово-экономической сферы в перспективе их подготовки к практическому применению технологий защиты информации и информационной безопасности, обозначают передовой уровень информационной культуры, необходимый будущим специалистам, чтобы быть конкурентоспособными на рынке труда.

5. Изучение университетской дисциплины «Информационная безопасность», посредством интернет-технологий и интерактивных методов, согласно исследованиям, помогает будущим специалистам финансово-экономической сферы решать различные

ситуации в профессиональной сфере. Этого можно достичь только путем постоянного развития материально-технической базы высшей школы, оснащения университетских центров современным электронным оборудованием, в том числе дидактико-научными материалами отечественного и зарубежного производства.

6. Университетская дисциплина «Информационная безопасность» является учебной дисциплиной, вносящей значительный вклад в профессиональную подготовку студентов финансово-экономической сферы, в том числе в развитие цифровых навыков и компетенций, что требует разработки и освоения новых подходов к обучению сквозь призму интерактивных методов. Таким образом, вопрос разработки новых стратегий обучения, выявления и применения интерактивных средств и методов обучения в области информационной безопасности является актуальным.

7. Принимая во внимание все вышеизложенное, сделан вывод, что актуальной является следующая проблема исследования, заключающаяся в определении теоретико-методологических основ повышения качества и эффективности изучения технологий защиты и безопасности информации с перспективы использования Интернет-технологий в профессиональной подготовке студентов финансово-экономической сферы.

8. Для решения проблемы исследования необходимо:

- научно обосновать внедрение информационных технологий, в том числе интернет-технологий, в процесс обучения технологиям обеспечения информационной безопасности будущих специалистов финансово-экономической сферы;
- разработать и усовершенствовать учебно-методический комплекс по вузовской дисциплине «Информационная безопасность» с внедрением интернет-технологий;
- сформировать педагогическую модель обучения технологиям обеспечения информационной безопасности будущих специалистов финансово-экономической сферы посредством интернет-технологий, в которой учесть требования рынка труда и основные педагогические и дидактические принципы;
- подтвердить посредством педагогического эксперимента эффективность предложенной педагогической модели и обосновать теоретические и методологические ориентиры применения педагогической модели.

2 ПЕДАГОГИЧЕСКАЯ МОДЕЛЬ И МЕТОДОЛОГИЯ ОБУЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ ЭКОНОМИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

2.1 Кибернетический подход при обучении информационной безопасности

Преподавание дисциплины «Информационная безопасность» студентам экономических и финансовых специальностей имеет ряд особенностей, связанных с динамизмом развития данного направления, ограничением аудиторного формата обучения, различным уровнем знаний и опыта применения информационных технологий обучающимися. Полученные в результате освоения дисциплины «Информационная безопасность» знания, умения и навыки, помогают в будущей профессиональной деятельности экономиста при работе с информацией, относящейся к категории коммерческой, служебной или государственной тайны. Поэтому важным является выбор педагогических технологий, позволяющих преподавателю оптимизировать учебный процесс для формирования компетенций в области информационной безопасности, выявить междисциплинарные связи. На наш взгляд, применение кибернетического подхода при моделировании педагогического процесса такого динамичного направления как информационная безопасность помогает повысить эффективность самого процесса обучения.

Понимание кибернетического подхода целесообразно начать с осмысления термина «кибернетика». Его в 1948 году впервые предложил американский математик, «отец кибернетики», Norbert Wiener в своей знаменитой книге «*Cybernetics: or the Control and Communication in the Animal and the Machine*» («*Кибернетика, или управление и связь в животном и машине*»). Анализируя результаты прикладных исследований различных научных направлений, ученый сделал вывод, что везде возникают одинаковые проблемы. Norbert Wiener поставил цель «*объединить усилия в различных отраслях науки, направить их на единообразное решение сходных проблем*» [103, с.8]. Если знать, как управлять системой, то она будет функционировать успешно. Сам автор теории определял кибернетику как «теория управления и связи в машинах и живых организмах» [104, с.56].

---

[103] НОВИКОВ, Д.А. *Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития*. Москва: ЛЕНАНД, 2016. 160 с. ISBN 978-5-9710-2549-8.

[104] ВИНЕР, Н. *Кибернетика или управление и связь в животном и машине*, 2-е изд. Москва: Советское радио, 1968, 328 с.

Основные принципы, или как их иногда называют законы, кибернетики сформулированы в разное время такими учеными как Уильям Эшби и Стаффорд Бир . На основе работ [105], [106], [107] построена схема принципов кибернетики (рис. 2.1).

Рис. 2.1. Принципы кибернетики

Как видно из схемы, описанные в середине прошлого века принципы кибернетики, можно применить в описании любой сложной системы. Например, изучение дисциплины «Информационная безопасность» студентами экономических специальностей также можно рассмотреть с помощью категорий и принципов кибернетики.

---

[105] ФЕДОСЮК, Я. В. Закономерности и принципы кибернетики как теоретико- методологическая основа формирования управленческих команд. В: *Сетевой научно-практический журнал Научный результат. Социология и управление*. 2015, №3, с. 89-92. ISSN 2408-9338.

[106] КАШИНА, О. А. О реализации общих принципов кибернетики в инновационном развитии инженерного вуз. В: *Образовательные технологии и общество*. 2018, №3 (Т.21), с. 284-289. ISSN 1436-4522.

[107] ЕВСЕЕВА, Ю. И. Программная кибернетика: современное состояние и проблемы. В: *Известия высших учебных заведений. Поволжский регион. Технические науки*. 2017, № 3 (43), с. 48–59. ISSN 2072-3059.

Кибернетический подход в педагогике начали применять с 50-х годов XX-го века. Сначала в виде программированного обучения, предложенного Skinner B. F. В своей книге «*The Technology of Teaching*» (1968) ученый пишет: «Simply leading the student through a solution in the traditional way is one kind of programming» (Простое ведение ученика через решение традиционным способом – это один из видов программирования) [108, с.102]. Говоря о программированном обучении, Skinner поясняет, что квалифицированный педагог видит, когда ученик готов перейти к следующему этапу в обучении. Иначе студент остается на одном и том же этапе до тех пор, пока не будет готов перейти к другому [там же, с.205]. Принцип программированного обучения перекликается с кибернетическим принципом обратной связи, при отсутствии которой невозможно управлять такой сложной системой как образовательный процесс.

В советской педагогике к принципам кибернетики обращались Колмогоров А. Н., Ительсон А. Б., Берг А. И., Архангельский С. И., Беспалько В. П., Федоров Б. И., Бабанский Ю. К., Болтянский В. Г., Блауберг Н.В., Садовский В.Н., Юдин Э.Г. и другие [109, с. 51].

Используя системный подход, кибернетика позволяет анализировать и управлять сложными процессами, учитывая взаимосвязи между частями системы, а также внешнего воздействия на нее, в плане принятия оптимальных решений для достижения поставленной цели. Кибернетический подход помогает эффективно анализировать и управлять процессом обучения для получения наилучших результатов благодаря механизмам и средствам аппарата исследования и моделирования сложных систем. Развитие информационных технологий способствует накоплению, передаче и обработке информации, делая более эффективным анализ процесса обучения и принятие решений для получения запланированного результата.

Для применения кибернетического подхода в управлении процессом обучения дисциплине «Информационная безопасность» необходимо определить цель и задачи обучения, уровень начальных знаний, умений и навыков студентов экономических специальностей, выбрать формы и методы организации учебного процесса для получения максимального результата при минимальных затратах, применить информационные и интернет-технологии для управления процессом обучения (рис. 2.2).

---

[108] SKINNER, B. F. *The Technology of Teaching.* New York: Appleton-Century-Crofts.1968, 255 с.

[109] ЧИБАКОВ, А.С. Кибернетический подход в обучении: историко-эволюционный и сущностный аспекты. В: *Technical Science / «Colloquium-journal».* 2019, №27 (51), с. 49-53. ISSN 2520-6990

Рис. 2.2. Кибернетический подход в преподавании ИБ будущим экономистов

***Разработано автором**

При определении цели и задач обучения дисциплин «Информационная безопасность», учитывались требования, предъявляемые к экономическим кадрам рынком труда, стандарты подготовки бакалавров направления 38.03.01 «Экономика» и принципы Болонского процесса [110].

Целью дисциплины «Информационная безопасность» является формирование у студентов устойчивых навыков работы в сложной сетевой информационной среде современного предприятия, офиса с учетом основных требований информационной безопасности.

Основные задачи дисциплины «Информационная безопасность»: получение сведений о современном состоянии проблем обеспечения информационной безопасности компьютерных систем, существующих угрозах, видах обеспечения ИБ, методах и средствах защиты информации, основах построения комплексных систем защиты, основ правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизмов их реализации, понятий и видов защищаемой информации.

Дисциплина «Информационная безопасность» относится к дисциплине по выбору вариативной части ООП ВО по направлению подготовки бакалавров 5.38.03.01 Экономика.

Процесс изучения дисциплины «Информационная безопасность» для студентов экономического направления подготовки направлен на формирование компетенций,

[110] *Портал Федеральных государственных образовательных стандартов высшего образования*, НИТУ «МИСиС». ©2021 [citat 28.12.2021]. Доступен: http://fgosvo.ru/fgosvo/92/91/4/88 /.

определенных в ФГОС ВО РФ по напарвлению 38.03.01 «Экономика»:

Общепрофессиональная компетенция ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Профессиональная компетенция ПК-10: способность использовать для решения коммуникативных задач современные технологические средства и информационные технологии.

С учетом требований Стандарта, рынка труда и разработанной схемы курса, считаем, что в результате изучения дисциплины «Информационная безопасность» студент должен:

Знать:

– нормативные и законодательные акты в области защиты информации;

– угрозы информационной безопасности;

– формальные и неформальные средства защиты информации;

– методы идентификации и аутентификации пользователей;

– принципы создания электронной цифровой подписи, алгоритмы хеширования;

– методы симметричного и ассиметричного шифрования;

– системы защиты от вредоносного ПО.

Уметь:

– анализировать источники угроз и каналы утечки информации;

– применять наиболее эффективные методы и средства защиты информации,

– проектировать организационные мероприятия по защите информации;

– контролировать эффективность мер защиты.

Владеть, иметь опыт:

– терминологией в области информационной безопасности;

– технологией противодействия угрозам информационной безопасности;

– защиты информации от компьютерных вирусов и вредоносного программного обеспечения,

– навыками выбора и настройки программных средств защиты информации;

– интерпретации результатов и анализа данных системных журналов средств защиты.

Согласно учебному плану изучение дисциплины «Информационная безопасность» предусматривает лекционные, практические занятия, организацию самостоятельной

работы студентов.

Особенность поставленных цели, задач, требований к знаниям, умениям и навыкам состоит в том, что в течение одного семестра и небольшого количества аудиторных занятий достаточно сложно охватить весь спектр направлений информационной безопасности. Но решению данной задачи благоприятствуют такие факторы как:

– наличие у обучающихся опыта использования информационных технологий;

– изучение информатики в школе и на первом курсе вуза;

– применение новых педагогических технологий и информационное обеспечение образовательного процесса;

– представление учебной информации в различных видах (графическая, аудио, видео);

– активизация самостоятельной деятельности студентов;

– сотрудничество преподавателя и обучающихся.

В рамках дисциплины «Информационная безопасность» необходимо на протяжении всего периода обучения возбуждать интерес к данной дисциплине. С первого же занятия студентам следует рассказать о кардинальных изменениях, происходящих в экономике, о ее цифровизации, преимуществах и связанных с ней угрозах. Рассмотреть такое явление как цифровая грамотность и цифровое неравенство, определить роль ИБ в этих процессах. Рассмотрение Стратегий и Концепций ИБ крупнейших государств мира помогает осознать значимость знаний и умений применения средств защиты информации не только в практической деятельности экономиста, но и в ежедневной практике каждого человека.

Необходимо также сообщить студентам, что компетенциям в области ИБ отведено особое место в Европейской рамке компетенций, в Российском Индексе Цифровой грамотности, в Концепции информационной безопасности Республики Молдова. ИБ и защита компьютерной информации давно стала частью информационных технологий, ее основы необходимо изучать, начиная со школьной скамьи, и повышать свою компетентность на протяжении всей жизни.

Применяя кибернетический подход, можно корректировать тематику теоретических и практических работ, дидактические методы, учитывая входной уровень знаний студентов экономических специальностей в области информационной безопасности и анализируя информацию, получаемую по обратной связи в процессе обучения.

На наш взгляд, проектирование занятий при обучении ИБ будущих экономистов в

условиях ограничения аудиторного времени и большого количества учебной информации с точки зрения кибернетического подхода позволяет повысить качество обучения. И так как при кибернетическом подходе изучают систему, в которой протекают информационные процессы по хранению и переработке информации, используемую для управления и регулирования, построим педагогическую модель по обучению дисциплине «Информационная безопасность» студентов экономических специальностей при помощи системного подхода.

2.2 Системный подход при моделировании процесса обучения

2.2.1 Общее понятие системного подхода

Системный подход приобретает все большее значение в различных областях человеческих знаний. О значимости системного подхода академик Асмолов А. Г. пишет *«Среди общенаучных принципов познания мира, выводящих за рамки построения картины действительности в конкретных дисциплинах, в том числе и в разных областях человекознания, все большее значение приобретает системный подход. Этот подход …зарекомендовал себя во многих науках. К нему обращаются исследователи, когда возникает задача синтеза различных знаний, выражающих общее стремление исследователей к созданию целостной картины явления или процесса. По своему месту в иерархии уровней методологии науки системный подход выступает как связующее звено между философской методологией и методологией конкретных наук»* [111, с. 76]. С 40-х годов XX века стал общенаучной методологией познания в различных дисциплинах.

В переводе с греческого система (σύστημα) – это целое, составленное из частей, соединение. Существует множество определений понятия «система», и практически во всех говорится о совокупности взаимосвязанных элементов, о таких свойствах систем как целостность, структурность, взаимосвязь, иерархичность, множественность описания. В работе советского и российского философа Садовского В. Н. «Основания общей теории систем» определено, что система – это «множество взаимосвязанных элементов, выступающее как определенная целостность» [112, с. 18]. Система – набор закономерно связанных элементов [113, с. 7].

Общие характеристики «системы» сформулированы в работе Асмолова А. Г. (рис.

---

[111] АСМОЛОВ А. Г. *Психология личности: культурно-историческое понимание развития человека.* 3-е изд. Москва: Смысл: Издательский центр «Академия», 2007. 528 с. ISBN 978-5-89357-221-6.
[112] САДОВСКИЙ, В. Н. *Основания общей теории систем*. Москва: Наука, 1974, 280 с.
[113] БЛИНКОВ, Ю.В. *Основы теории информационных процессов и систем*: учеб. пособие. Пенза: ПГУАС, 2011. 184 с. ISBN 978-5-9282-0725-0.

2.3).

Рис. 2.3. Характеристики системы по Асмолову А. Г.

При исследовании систем строят модели, помогающие изучить имеющуюся структуру и взаимосвязи:

1) модель «черного ящика»;

2) модель состава системы;

3) модель структуры системы [114, с. 10].

Системный подход применяется при изучении сложных систем, к которым, несомненно, можно отнести и исследования в области педагогики.

Рассмотрим процесс обучения информационной безопасности будущих экономистов с точки зрения теории систем. Построим все три вида моделей, выделив наиболее значимые, с точки зрения нашего исследования, элементы и связи.

2.2.2 Модель «черный ящик»

С точки зрения системного анализа любой объект можно исследовать с позиции «черного ящика». В основе построения модели «черный ящик» лежат такие свойства системы как «целостность» и «обособленность от среды». Система связана с внешней средой: внешняя среда воздействует на систему и система воздействует на внешнюю среду. Обозначим стрелками входы и выходы системы. Выход системы в данной модели соответствует слову «цель» в словесной модели. Связи могут быть вещественными,

[114] БЛИНКОВ, Ю.В. *Основы теории информационных процессов и систем.* Пенза: ПГУАС, 2011. 184 с. ISBN 978-5-9282-0725-0.

энергетическими, информационными. При этом, как организована сама система, на этапе построения модели, нас не интересует [[115]с.44, [116]с.14].

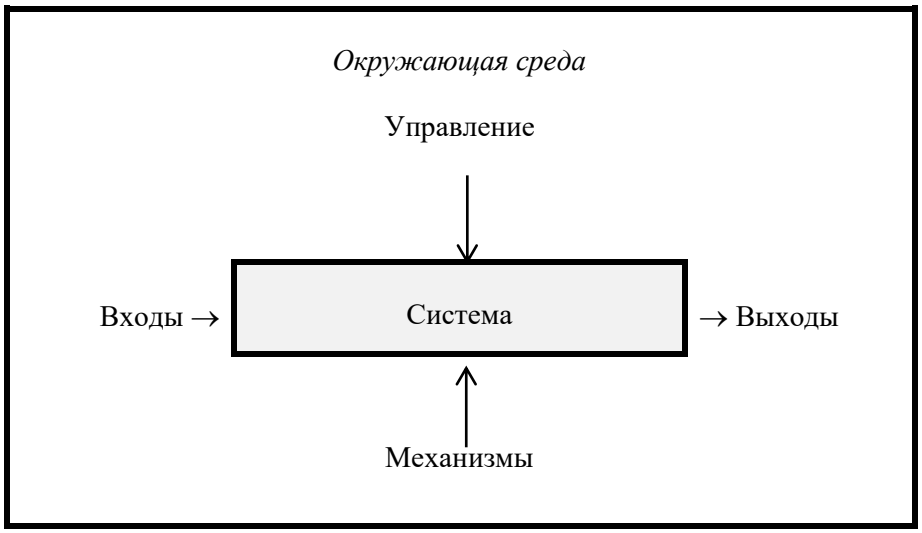


Рис. 2.4. Модель системы «черный ящик»

Образовательный процесс относится к классу сложных систем, состоит из множества подсистем, элементов и управляющих воздействий. Если представить процесс обучения студентов информационной безопасности в виде модели «черный ящик», то необходимо определить входы (ресурсы либо входную, оперативную, информацию), выходы определяют произведенные при выполнении функции результаты (данные, выходную информацию). Управление – предписывающая или ограничивающая информация (инструкции, законы, руководства, методики и т.п.), сведения о том, при каких условиях, по каким правилам (как, где, когда) выполняется функция. Механизмы определяют все то, с помощью чего выполняется функция, т. е. осуществляется преобразование входа в выход. К механизмам относят ресурсы, оборудование, кадры.

Рассмотрим процесс обучения информационной безопасности будущих экономистов в вузе в виде модели «черный ящик» (табл. 2.1)

[115] ГРОМОВ, Ю. Ю., ДИДРИХ, В. Е., ИВАНОВА, О. Г., ОДНОЛЬКО, В. Г. *Теория информационных процессов и систем*. Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2014. 172 с. ISBN 978-5-8265-1352-1.
[116] 72. ИВАНОВ, И. В. *Теория информационных процессов и систем*. 3-е изд. Москва: Издательство Юрайт, 2018. 228 с. 978-5-534-05705-8.

Таблица 2.1. О сложностях обучения информационной безопасности (ИБ) будущих экономистов в вузе

Вход	Уровень информационной культуры, включающий в себя элементы ИБ	Знания, полученные в школе, в вузе на занятиях по информатике		Управление				Выход (Цель)	Компетенции в области ИБ	ЗУН в области правовых, организационных, социальных, технических, программных, математических средств защиты информации
				Стандарт обучения в вузе	**Требования рынка труда**	**Потребности общества**				
				Федеральный Государственный Образовательный Стандарт РФ ВО по направлению подготовки 38.03.01 Экономика, утвержден 12.11.2015 Общепрофессиональная компетенция (ОПК-1): способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	– клиентоориентированность; – приверженность к работе; – умение работать в команде; – склонность к обучению; – умение и желание учиться; – способность брать на себя ответственность; – самостоятельность; – умение решать нестандартные задачи; – работоспособность; – умение планировать свою деятельность; – ориентация на достижение результата; – аналитическое мышление; – инициативность; – предприимчивость; – самоуправление; – дисциплинированность; – коммуникативность; – самопрезентация; –умение работать в условиях многозадачности и с большим объемом информации; – адекватность личностной и профессиональной самооценки.[117]	Недопущение вреда от опасных информационных воздействий на психическое, нравственное или физическое состояние личности[118]			
			→	↓	↓	↓				
				ОБУЧЕНИЕ ИБ БУДУЩИХ ЭКОНОМИСТОВ			→			
				↑	↑					
				Литература для технических специальностей Литература по защите офисных документов	Специалист в области информационных технологий, обладающий знаниями в области экономики, права, математики, психологии и т.п.					
				Учебно-методическая литература	**Уровень подготовки преподавателя**					
				Механизмы						

[117] ГЛОТОВА Е.Е. Требования работодателей к выпускникам вузов: компетентностный подход. В: *Человек и образование*. 2014, № 4 (41), с.185-187. ISSN 1815-7041.
[118] ПОЛЯКОВ, В.П., РОМАНЕНКО, Ю.А. Педагогическое сопровождение вопросов информационной безопасности личности в отечественном образовании. В: *Труды Международного симпозиума «Надежность и качество»*. 2018, том 1, с. 64-67. ISSN 2220-6418.

Входом будет некоторый уровень знаний и умений студента в области информационной безопасности, полученный в процессе обучения в школе, на занятиях по информатике в вузе. Очевидно, что входной уровень у всех студентов может быть разный, обусловленный разницей в начальном уровне подготовки.

На *выходе* (после прохождения курса «Информационная безопасность») у студента должна быть сформирована компетенция в вопросах защиты информации. Это набор навыков, умений и знаний по идентификации и оценке угроз информационной безопасности; применению правовых, организационных, программных, технических методов и средств защиты информации; защите электронных документов; основам криптографических методов сокрытия информации; основам применения электронно-цифровой подписи.

На процесс подготовки оказывает влияние внешняя среда. Выделим управляющие факторы и механизмы воздействия на систему подготовки будущих экономистов в области информационной безопасности.

К *управляющему воздействию* отнесем стандарт обучения, требования рынка труда, потребности общества.

У будущих экономистов, согласно утвержденного 12 ноября 2015 года Федерального Государственного Образовательного Стандарта Высшего образования Российской Федерации подготовки бакалавров по направлению 5.38.03.01 «Экономика», должна быть сформирована общепрофессиональная компетенция ОПК-1: «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности».

Среди требований работодателей к будущим выпускникам, можно выделить умение работы с большим объемом информации. Очевидно, при соблюдении ее целостности, конфиденциальности и доступности.

Общество также предъявляет повышенные требования к обеспечению прав личности в информационной среде неразрывно связанных с вопросами информационной безопасности. Об этом говорится в государственных Стратегиях и Доктринах по информационной безопасности, принятым, практически, в каждом государстве.

К *механизмам,* оказывающим влияние на процесс подготовки будущего экономиста в области защиты информации, можно отнести учебно-методическую литературу и самого преподавателя. Изученная учебная литература в области защиты информации чаще всего узкоспецилизирована, предназначена для подготовки в вузе технических специальностей. В качестве примера, приведем таких авторов как Бондарев

В. В., Блинов А. М., Зима В. М., Молдовян А. А., Емельянова Н. З., Партыка Т. Л., Попов И. И., Игнатьев В. А., Каторин Ю. Ф., Разумовский А. В., Спивак А. И., Курило А. П., Зефиров С. П., Голованов В. Б., Нестеров С. А., Малюк А. А., Пазин С. В., Погожин Н. С., Мельников В. П., Платонов В. В., Торокин А. А., Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф., Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В., Хореев А. А., Хорошко В. А., Ярочкин В. И. и др. В других источниках представлена информация по защите офисных документов, например в работах Корнеева И. К., Степанова Е. А.. Первый тип учебно-методической литературы достаточно сложен для студентов экономического профиля подготовки. Второй тип – не позволяет сформировать полный набор навыков, знаний и умений в области информационной безопасности, необходимых для современного экономиста.

Особые требования необходимо предъявить к компетенциям преподавателя. Он должен обладать знаниями в таких областях как информатика, экономика, математика, право, психология, социология и т.п. Чаще всего информационную безопасность будущим экономистам преподают специалисты в области информационных технологий, без экономического образования, делающие акцент на формальных способах защиты информации.

2.2.3 Модель состава системы

С помощью модели «черного ящика» невозможно описать внутреннее устройство системы. Внутренность «ящика» неоднородна, состоит из различных составных частей, каждая из которых так же может быть разбита на составные части и т.д. Неделимая часть системы называется в теории систем элементом. Подсистемой называется часть системы, содержащая в себе более одного элемента[119, с.10].

В системе обучения, или образовательном процессе принято выделять такие подсистемы и элементы как: цели, содержание, принципы, формы, методы, средства, диагностика результатов, а также педагог и обучаемый [120, с. 19].

Педагогическая система, являясь сложной, всегда обладает свойством иерархичности: наличия множества элементов, находящихся в отношении подчиненности низших уровней высшим. Выделим три ключевые с нашей точки зрения подсистемы:

– «преподавание»;

– «учение»;

– «оценивание».

---

[119] БЛИНКОВ, Ю.В. *Основы теории информационных процессов и систем*. Пенза: ПГУАС, 2011. 184 с. ISBN 978-5-9282-0725-0.

[120] ПОДЛАСЫЙ, И.П. *Педагогика: Теория и технологии обучения*. Москва: Гуманитар., изд. центр ВЛАДОС, 2007. 575 с. ISBN 978-5-691-01553-3.

В подсистеме «*преподавание»* отобразим такие подсистемы как лекционные, практические, лабораторные занятия.

Теоретический материл в области информационной безопасности является как узко специализированным, так и тесно связанным с другими дисциплинами. Сама дисциплина постоянно развивается, появляются новые направления исследований, такие как информационное право и киберэтика. Научная и учебно-методическая литература в области информационной безопасности охватывает такие направления как: техническая защита информации, организационно-правовые вопросы обеспечения информационной безопасности, программная защита информации, криптография, киберэтика (рис. 2.5). Исходя из вышесказанного и учитывая поставленные цели в обучении информационной безопасности специалистов экономического профиля для обеспечения соответствия содержательной части дисциплины определены теоретические разделы (Т):

Т1. Введение. Основные понятия и определения

Т2. Угрозы ИБ и каналы утечки информации

Т3. Правовые средства защиты информации

Т4. Организационные средства защиты информации

Т5. Физические и технические средства защиты информации

Т6. Программные средства защиты информации

Т7. Идентификация и аутентификация

Т8. Криптографические подходы к защите информации и электронно-цифровая подпись

Т9. Морально-этические средства защиты информации

Лабораторные и практические занятия направлены на формирование практических навыков и умений в области информационной безопасности. В соответствии с этим определены и подготовлены задания к выполнению лабораторных (Л) и практических (П) работ по следующим темам:

Л1. Политика безопасности Windows

Л2. Оптимизация дискового пространства

Л3. Архивация

Л4. Парольная защита

Л5. Защита флеш-накопителей

Л6. Антивирусная защита информации

Л7. Защита текстовых документов

Л8. Защита электронных таблиц

П1. Методы симметричного шифрования

П2. Методы ассиметричного шифрования и ЭЦП

Составлена схема курса по обучению информационной безопасности, на которой представлены темы лекционных и лабораторных, практических занятий, направления самостоятельной работы студентов (рис. 2. 5).

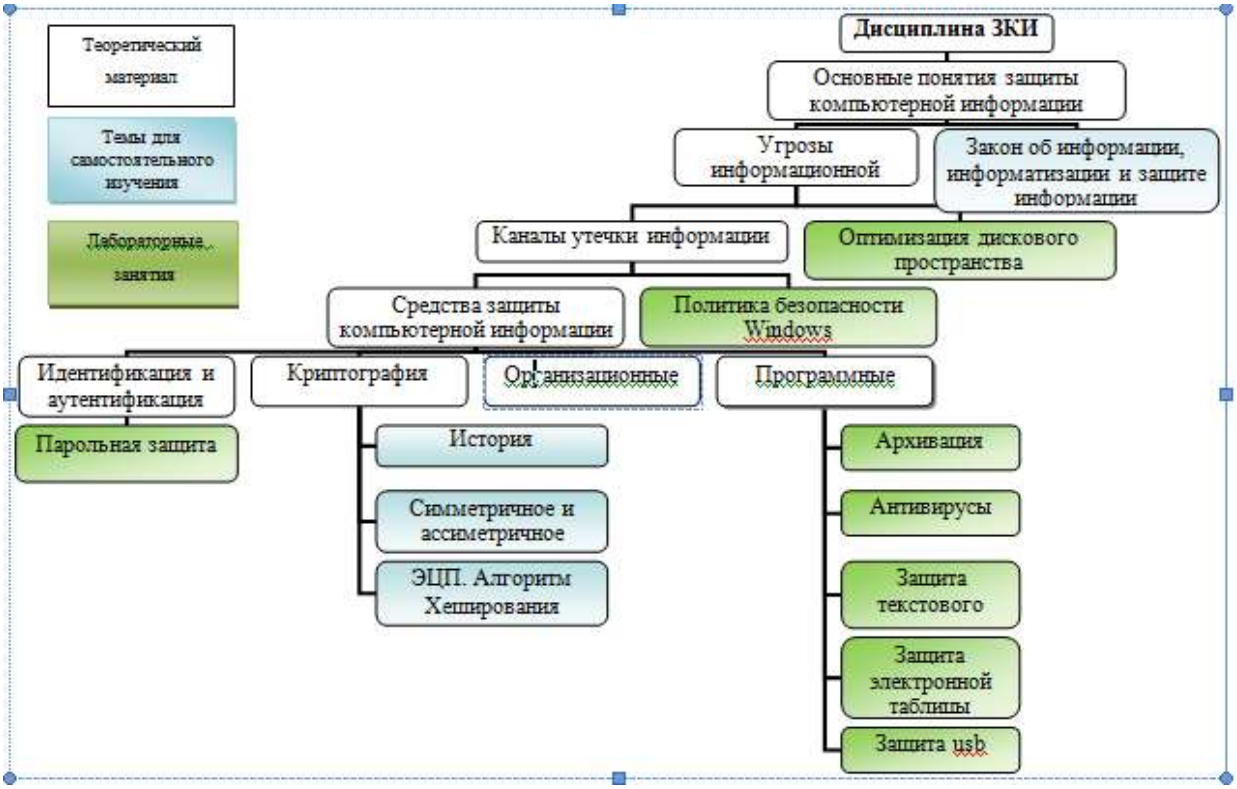


Рис. 2.5. Карта курса «Информационная безопасность»

В подсистеме «учение» важной частью является организация самостоятельной деятельности студентов. Согласно современным образовательным стандартам на самостоятельное обучение выделяется до 50% времени. Акценты на активизацию самостоятельной работы обучающихся стали выставлять со сменой парадигмы «Образование на всю жизнь» на парадигму «Образование в течение всей жизни». Планирование, организация и реализация самостоятельной работы студента является важной задачей процесса обучения в вузе.

К самостоятельным видам деятельности принято относить научную, учебную и социальную деятельность обучающегося.

Особое внимание в этой подсистеме уделено информационно-коммуникационным технологиям, способствующим поддержке реализации данного процесса:

– программа создания электронных учебников SunRav;

– программа создания интерактивных демонстраций PowerPoint;

– цифровая издательская платформа Joomag;

– инструменты Google: Google Sites, Google Forms;

– он-лайн конструктор тестов Testmoz.

В подсистеме «оценивание» выделены подсистемы, помогающие определить результативность процесса обучения основам информационной безопасности будущих экономистов:

– обучающий контроль;

– накопительная балльно-рейтинговая система;

– итоговое тестирование.

В результате получена упрощенная модель «состава системы» процесса обучения основам информационной безопасности студентов экономических специальностей (рис. 2.6).

Рис. 2.6. Модель «состава системы» – компоненты курса и применяемые ИКТ

На рисунке 2.6 представлены составные части системы обучения дисциплине «Информационная безопасность». Это и подсистемы преподавание – обучение – оценивание, состоящие в свою очередь из подсистемы и элементов, рассмотренных выше. А также информационно-коммуникационные технологии поддержки этих процессов.

В построенной модели «состава системы» не представлены некоторые обязательные элементы педагогического процесса: преподаватель и обучающийся, формы, методы и содержание, цели и результатов. Отразим их в дальнейшем при построении модели структуры системы.

2.2.4 Модель структуры системы

Для полного и всестороннего описания сложной системы недостаточно применения моделей «черный ящик» и «состава системы», так как в первом случае описывается окружение изучаемой системы, во втором – подсистемы и элементы. С

помощью модели «структура системы» описывают отношения (связи) между компонентами (подсистемами и элементами), необходимые для достижения цели функционирования системы.

Связи между компонентами системы могут быть энергетическими, информационными, вещественными. По направлению выделяют прямые и обратные связи. Графически связи принято обозначать одно или двунаправленными стрелками. Между объектами системы может быть бесконечное число связей, но для простоты моделирования принято указывать лишь существенные отношения между компонентами системы.

В предыдущих пунктах определено, что целью обучения основам информационной безопасности студентов экономических специальностей является формирование у них компетенций в данной области. В качестве факторов внешней среды выделены Стандарты обучения, квалификационные стандарты, требования рынка труда, учебно-методическая литература. В качестве элементов и подсистем определены подсистемы: преподавание, учение, оценивание; субъекты образовательного процесса: преподаватель и обучающийся; методы, формы и средства обучения; содержание дисциплины.

При построении модели обучения информационной безопасности будущих экономистов необходимо учесть взаимосвязи (отношения) между подсистемами и элементами, которые, с нашей точки зрения, существенны для достижения рассматриваемой цели. Для этого представим этот процесс в нотациях модели структуры системы, или педагогической модели.

2.2.5. Педагогическая модель

Применение моделирования в педагогике, как метода научного познания, многими исследователями признается сложным процессом, характеризующимся наличием: 1) множества объектов, в том числе скрытых от исследователя; 2) взаимозависимых, взаимодействующих элементов; 3) вероятностного характера природы педагогических явлений. В педагогической модели характеристики и свойства этого процесса в абстрактной форме выстраиваются в одну систему. Платонова Р. И., анализируя различные подходы ученых к применению метода моделирования, в научно - педагогических исследованиях утверждает, что «*моделирование позволяет конструктивно представить системность и процессуальность объектов педагогического процесса, отобразить их структуру и связь, дает возможность в ускоренном режиме проводить эксперименты, избежать существенных ошибок в*

разработке …новой концепции»[121 , с. 193].

Синтез выбранных подсистем и элементов, отражение их взаимосвязи позволяет построить адекватную модель обучения информационной безопасности будущих специалистов финансово-экономических специальностей с помощью современного и мощного аппарата теории систем и системного анализа (рис. 2.7.).

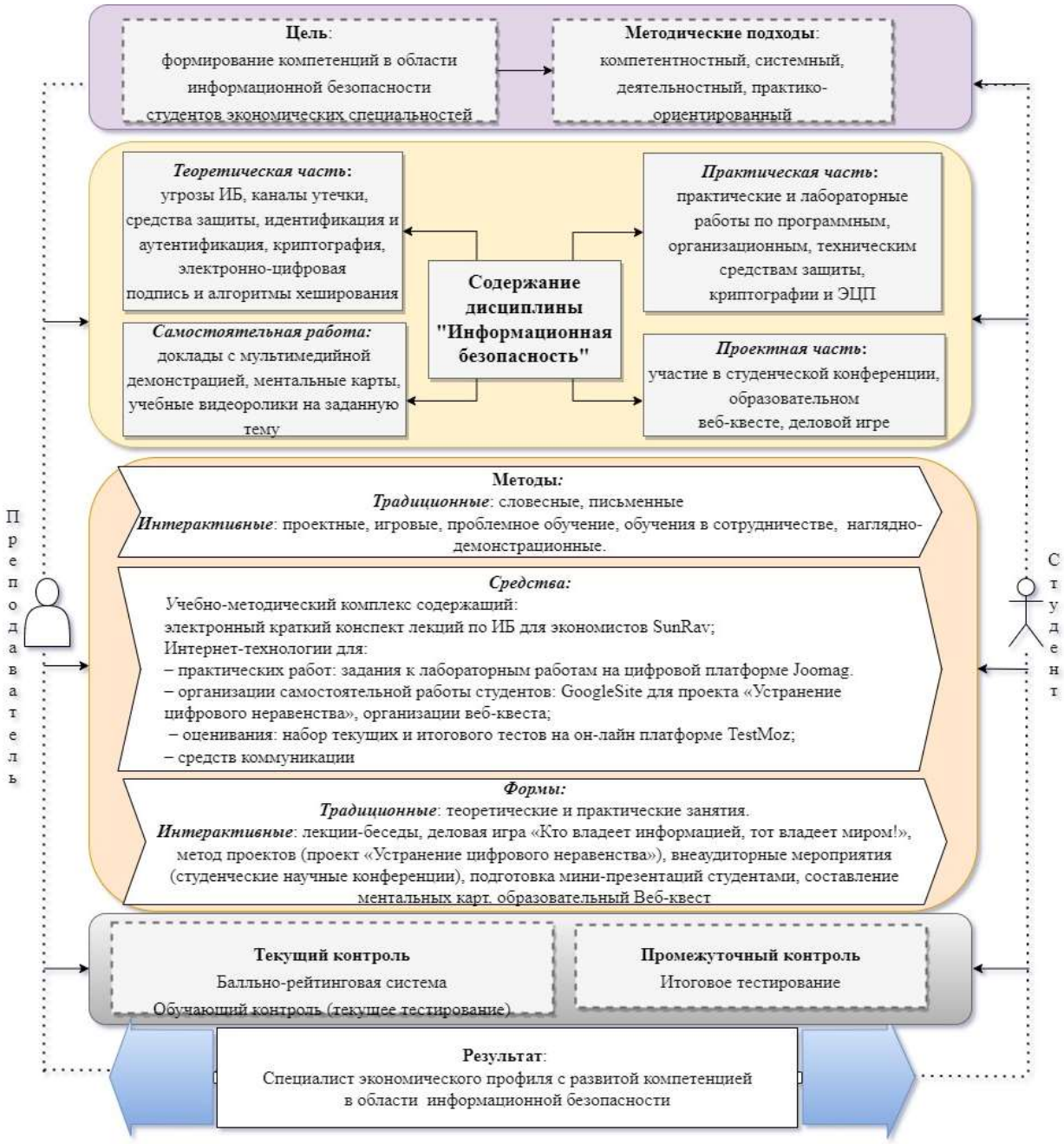


Рис. 2.7. Педагогическая модель

Отличительной чертой проектирования педагогической модели стало применение системного подхода. Изначально процесс обучения информационной безопасности

---

[121] ПЛАТОНОВА Р. И. Моделирование в научно – педагогических исследованиях. В: *Azimuth of Scientific Research: Pedagogy and Psychology*. 2017, Т. 6, № 3(20), с. 190-193. ISSN 2309-1754.

будущих экономистов был описан как модель «черного ящика», затем как модель «состава системы». Отражение связей между подсистемами и учет внешней среды позволили построить педагогическую модель в нотациях модели «структуры системы». Таким образом, педагогическая модель обучения основам информационной безопасности будущих специалистов финансово-экономической сферы отображает объект исследования с точки зрения системного подхода, помогает понять, как функционирует система.

Сам процесс разработки педагогической модели помог глубже понять процессы и явления, происходящие при обучении основам информационной безопасности будущих экономистов, и иметь возможность прогнозировать возможные направления развития.

Особенность разработанной педагогической модели состоит в том, что при формировании теоретической и практической части содержания обучения учтена взаимосвязь информационной безопасности с экономической. Соотнесение тем дисциплины с экономическими явлениями и процессами помогает обучающимся ответить на вопросы «что защищать?», «от кого защищать?», «как защищать?».

Педагогическая модель направлена на выявление междисциплинарных связей информационной безопасности с другими отраслями знаний, изучаемыми в вузе будущими специалистами финансово-экономической сферы. Практическая реализация заключается в применении интернет-технологий на всех этапах преподавание-учение-оценивание.

Междисциплинарные связи, влияние информационной безопасности на экономическую, – делают возможным добиться более качественного развития компетенций в области информационной безопасности будущим специалистам финансово-экономического профиля с перспективы интернет-технологий и личностно-ориентированного обучения.

В ходе педагогического эксперимента необходимо проверить эффективность построенной педагогической модели обучения информационной безопасности будущих экономистов.

2.3 Методология применения разработанной педагогической модели

2.3.1 Методические аспекты применения интернет технологии

Информационно-коммуникационные технологии, особенно интернет технологии, удобно использовать в обычном обучении, при организации самостоятельной работы в аудиторном и внеаудиторном формате, для студентов заочной формы обучения, в дистанционном обучении. На сегодняшний день существует множество он-лайн средств, с помощью которых педагог может подготовить учебно-методические материалы даже не владея навыками программирования. В таких средствах обычно можно использовать

наряду с текстовой информацией аудио и видео материалы, что повышает наглядность и, как следствие, усваиваемость новых знаний.

Особыми преимуществами учебных материалов созданных он-лайн средствами являются:

1) возможность оперативного внесения изменений, что особенно важно для дисциплины «Информационная безопасность»;

2) возможность быстрого получения информации с любого компьютера, устройства при наличии доступа к сети Интернет;

3) возможность размещения дополнительных материалов повышенной сложности для студентов, с более высоким уровнем информационной подготовки.

Для каждой, выделенной в ходе описанного выше системного проектирования, подсистемы процесса «преподавание» -– «учение» – «оценивание» дисциплины «Информационная безопасность» применяются различные информационно-коммуникационные средства и информационные сервисы сети Интернет.

Лекции представлены в виде демонстрационных материалов Power Point, видео записей, электронного краткого курса лекций, созданных в SunRav BookEditor. Материалы для практических работ представлены в виде демонстрационных материалов Power Point. Материалы для проведения лабораторных работ размещены на издательской интернет платформе Joomag. Для организации самостоятельной работы студентов на платформе GoogleSites создана образовательная страница, содержащая инструкции и материалы по веб-квесту. В проекте «Устранение цифрового неравенства» применяются GoogleForms, GoogleTables и другие средства сервиса Google. Диагностическим инструментарием оценивания знаний студентов выбран он-лайн конструктор тестов Testmoz, позволяющий не только создавать вопросы различного типа, но и всесторонне оценивать результаты. Характеристика применяемых интернет-технологий представлена в Приложении 4.

Наряду с традиционными лекциями, лекциями-дискуссиями важно проводить лекции-конференции. Например, на лекции-конференции «Служебные тайны», в рамках раздела «Правовые средства защиты информации», студенты выступают с краткими докладами (четыре слайда: титульный, определение, статьи законов, реальный пример наказания за разглашение служебной тайны) на одну из тем «Тайна…»: коммерческая, банковская, адвокатская, суда и следствия, нотариальная, усыновления и т.д. В заключение подводится итог, что нарушение служебной тайны в современном мире чаще всего происходит с помощью информационных технологий. Студенты видят взаимопроникновение права, экономики и информационных технологий, а также

неразрывную связь с ИБ.

На лекции-конференции «Вредоносное программное обеспечение и принципы его работы», в рамках раздела «Программные средства защиты информации», студенты выступают с краткими докладами (4 слайда: титульный, определение, алгоритм действия, реальный пример осуществления) по следующим темам: Вирусы, Сетевые черви, Трояны, Вирусы-шпионы, Клавиатурные шпионы, Спам, Фишинг, Рекламное ПО, Программы скрытого дозвона, Макровирусы, Почтовые вирусы, Похитители паролей, Дропперы, Загрузочные вирусы и т.д. Такие лекции помогают студентам развивать и улучшать коммуникативные навыки, получать опыт публичных выступлений.

При изучении дисциплины «Информационная безопасность» студентам предлагаются по вызывающим сложность темам подготовленные видео лекции. Видеолекция, как продукт образовательного процесса помогает обучающимся самостоятельно освоить новый материал или повторить пройденный. На самостоятельную проработку вынесены отдельные темы, которые не успеваем изучить в аудиторном формате. В ходе видеолекции ставятся вопросы, которые затем обсуждаются в аудиторном формате, таким образом, студенты вынуждены не только посмотреть видео лекцию, но и подготовить ответы. Особые преимущества видеолекции предоставляют на практических занятиях. Студенты могут их пересмотреть и выполнить практическое задание в удобном темпе.

Благодаря такой концентрации теоретического материала, разнообразию практических работ, у студентов формируется более полное представление об обеспечении защиты информации в рамках профессиональной деятельности экономистов.

2.3.2 Методические аспекты организации проектной деятельности студентов

Метод проектов относится к новым педагогическим технологиям, хотя появился в начале XX века в США. Впервые проектный метод описал William Heard Kilpatrick, ученик американского философа и педагога John Dewey, в работе «The project method» (1918). Для проектного метода характерно рациональное сочетание теоретического материала и его практического применения в решении конкретных проблем при индивидуальной или групповой работе обучающихся [122, с. 65].

Теоретические основы проектного обучения, а также возможность применения при организации самостоятельной работы рассмотрены в работах William Heard Kilpatrick [123],

---

[122] ПОЛАТ, Е. С. Новые *педагогические и информационные технологии в системе образования*. Москва: Издательский центр «Академия», 2003. 272 с. ISBN 5-7695-0811-6.
[123] KILPATRICK, W. H. *The Project Method. Teachers College Record*, 1918. 320 p.

В.П. Беспалько, И. В. Богданова, В.В. Гузеева, В.В. Давыдова, Я. Дитриха, Д. Дьюи, В. Килпатрика, В.М. Монахова, Н.Ю. Пахомовой, Е.С. Полат, И.Д. Чечель и др.

Sorin Creastea, пишет, что в румынской педагогике проект рассматривается как: а) метод обучения, основанный на действиях (исследовательский, учебный, конструкторский, проблемный и т. д.); б) модель «интегрированного обучения», основанного на междисциплинарности и трансдисциплинарности. Ученый подчеркивает, что проектное обучение должно быть интегрировано в педагогическом контексте взаимозависимых педагогических систем «преподавание – обучение – оценивание»[124 , с. 58]

Технология проектной деятельностью эффективна для организации самостоятельной работы в аудиторном и внеаудиторном формате, помогает развивать творческие способности, умение работать в группе и навыки критического мышления. Эти посылы видим в определении проектного метода и проектной технологии в работе профессора Полат Евгении Семеновны «Новые педагогические и информационные технологии в системе образования»: а) «*как метод предполагает определенную совокупность учебно-познавательных приемов, которые позволяют решить ту или иную проблему в результате самостоятельных действий учащихся с обязательной презентацией этих результатов*»; б) «*как педагогическая технология включает в себя совокупность исследовательских, поисковых, проблемных методов, творческих по самой своей сути»* [*125*, с. 63].

Проектная технология имеет четкую последовательность этапов, в рамках которых применяются проблемные, поисковые, исследовательские методы с одной стороны и интеграция знаний и умений из различных дисциплин, а также применение творческих способностей обучающихся другой стороны.

Этапы учебного проекта и краткая содержательная характеристика, описанные в [126, с. 30], представлены на схеме (рис. 2.8).

---

[124] CRISTEA, S. *Instruirea prin proiecte*. În: *Didactica Pro*. 2018, nr. 1(107), p. 57-60. ISSN 1810-6455.

[125] ПОЛАТ, Е. С. *Новые педагогические и информационные технологии в системе образования*. Москва: Издательский центр «Академия». 2003. 272 с. ISBN 5-7695-0811-6.

[126] ДАУТОВА, О. Б., ИВАНЬШИНА, Е. В., ИВАШЕДКИНА, О. А., КАЗАЧКОВА, Т. Б., КРЫЛОВА, О. Н., МУШТАВИНСКАЯ, И. В. *Современные педагогические технологии основной школы в условиях ФГОС*. Санкт-Петербург: КАРО, 2015. 176 с. ISBN 978-5-9925-0890-1.

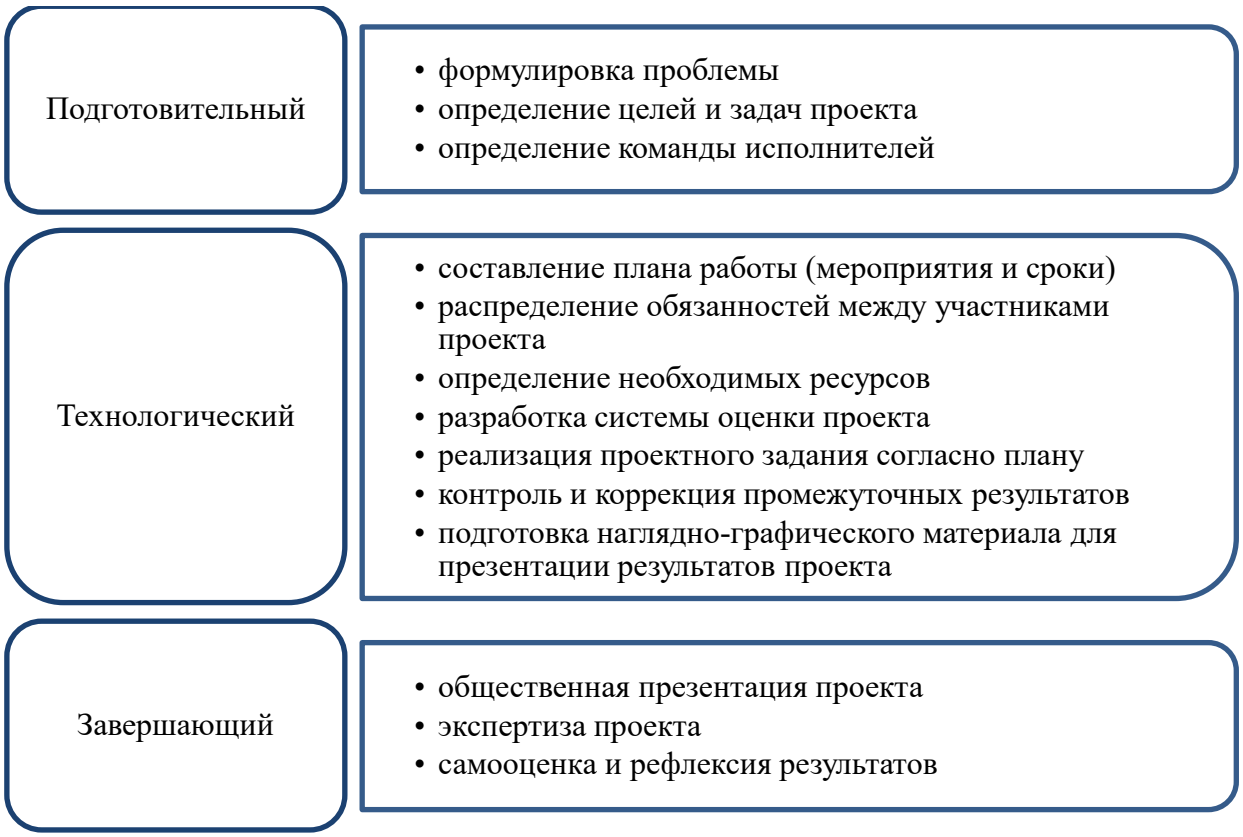


Рис. 2.8. Этапы учебного проекта

Учебный проект при обучении дисциплине «Информационная безопасность» студентов экономических специальностей позволяет расширить тематику курса, развить творческие способности студентов, активизировать самостоятельную деятельность, улучшить навыки коммуникации и групповой работы. Сегодня существует множество различных подходов к организации проектной деятельности, внедряемых в образовательный процесс всех ступеней, начиная от дошкольного образования и заканчивая послевузовским образованием. Популярность применения данной педагогической технологии кроется в возможности применение фактических знаний и приобретение новых, в том числе благодаря самообразованию [Шибкова, с. 212].

К классу проектных методов можно отнести технологию образовательного Web - квеста, впервые предложенного в 1995 году американским профессором образовательных технологий государственного университета в Сан-Диего Bernie Dodge [127].

Web-квест многие исследователи рассматривают как проект, либо как проблемное задание, информационные источники для выполнения которого находятся в сети Интернет (Воробьёв Г.А.). Багузина Е. И. трактует как Web-квест как проблемное задание с элементами ролевой игры, для выполнения которого используются ресурсы сети Интернет. Напалков С. В. понимает под тематическим образовательным Web -квестом

[127] Dodge B. *Some Thoughts About WebQuests*. - URL: http://webquest.sdsu.edu/about_webquests.html (дата обращения: 25/09/2018).

выполнение учащимися поисково-познавательных заданий с использованием Интернет-ресурсов по учебной теме в соответствии с целями и задачами ее изучения для систематизации и обобщения изученного материала [128, с.11-12].

В зависимости от образовательной цели выделяют:

– краткосрочный веб-квест (1-3 дня) направлен на поддержку приобретенных знаний;

– долгосрочный веб-квест (более 3 дней) направлен на расширение и улучшение приобретенных знаний.

Любой веб-квест состоит из следующих элементов:

1) ***введение***, в котором приведены исходные данные;

2) заранее разработанное ***задание***, состоящее, как правило, из подзадач;

3) ***сеть*** информационных ресурсов, необходимых для выполнения задач (ссылки на ресурсы WorldWideWeb или прилагаемые документы);

4) объяснение обучающимся ***процесса*** прохождения этапов;

5) некоторые ***рекомендации*** (в виде инструкций, ментальных карт или диаграмм) по организации данных;

6) ***выводы*** позволяют учащимся сравнить полученный результат с поставленной целью, иногда расширить свой опыт в других областях (Dodge, 1997) [129 , с.4].

Web-квест позволяет организовать самостоятельную работу обучающихся по поиску актуальной, безопасной и адекватной информации во Всемирной паутине по конкретной тематике для исключения ситуации, когда учащийся сталкивается с огромным объемом информации и не может определить ее релевантность. Более того подготовка к веб-квесту в группе помогает развить навыки командной работы, углубить и расширить получаемые на теоретических и практических занятиях знания [130, с.134-138].

В рамках изучения дисциплины «Информационная безопасность» для студентов экономических специальностей разработан образовательный Web-квест по теме «Криптография». Общее направление работы, этапы и основные элементы представлены на рисунке 2.9 .

---

[128] НАПАЛКОВ, С.В. *Тематические образовательные Web-квесты как сред-ство развития познавательной самостоятельности учащихся при обучении алгебре в основной школе*. Автореф. дис. ... канд. пед. наук. Саранск, 2013. 26 с.

[129] PERIZAT, B., SEITKAZYA. A Web-Quest as a Teaching and Learning Tool IEJME. In: *Mathematics Education*, 2016, Vol. 11, No 10, Ankara: Turkey, p. 3537-3549.

[130] ДАРИЕНКО, М.С., БОГДАНОВА, В.А. Возможности интеграции Web-квест технологии на этапе обобщения и систематизации знаний обучающихся. В: *Общекультурные и естественнонаучные аспекты образования в интересах устойчивого развития: сборник статей участников Международной научно-практической конференции (25 ноября – 3 декабря 2018 г.)* / Отв. ред.С.В. Напалков. –Арзамас: Арзамасский филиал ННГУ, 2018. 275 с.

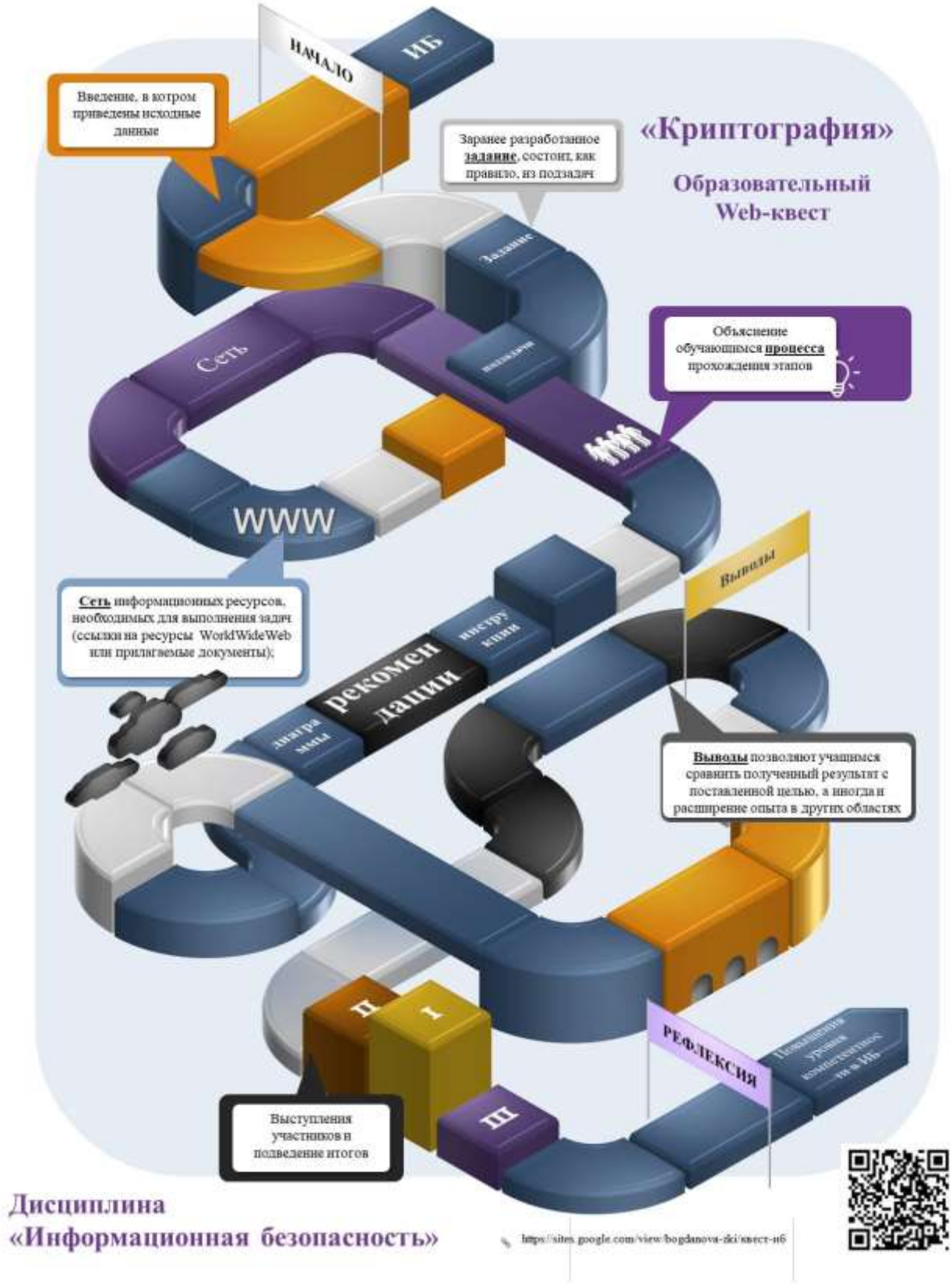


Рис. 2.9. План организации образовательного web-квеста по ИБ

Содержательные компоненты, охватывающие теоретический материал, практические навыки, роли, учебные действия обучающихся представлены в таблице 2.2.

Таблица 2.2. Примеры заданий для обобщающего занятия по теме «Основы криптографии» в рамках дисциплины «Информационная безопасность»

Тема: «Криптография»				
Содержательные компоненты темы	Роли	Учебные действия обучающегося		
		узнать	создать	оформить
Теоретический материал	I. ТЕОРЕТИК Цель: систематизировать теоретические сведения о криптографических методах	- определения понятий, используемых в криптографии; - какие стандарты шифрования используются в современном мире?	- тезаурус темы «Криптографические методы»; - опорный конспект темы «Современные криптографические методы».	(электронный ресурс)
Практический материал	II. ПРАКТИК Цель: изучить приложения криптографических алгоритмов	- прибегает ли человек в повседневной жизни к криптографии? - в каких сферах деятельности человеку приходится применять криптографию?	- карту приложений криптографии; - подборку прикладных криптографических задач	(электронный ресурс)
Исторические ошибки	III. ИСТОРИК Цель: изучить историю развития криптографических методов	- зачем людям понадобилось шифровать информацию? - когда и как люди начали шифровать и расшифровывать информацию? - кто из учёных математиков создал криптографические алгоритмы ?	- хронологию криптографических методов; - галерею создателей криптографических методов; - библиографию научных трудов, посвящённых криптографии.	(электронный ресурс).
Возможные ошибки учащихся	IV. ОШИБКОВЕД Цель: систематизировать проблемы, которые возникают при шифровании информации	- распространённые проблемы при сокрытии информации; - заблуждения (недоразумения), возникающие при сокрытии информации.	- банк заданий по криптографии; - памятку «Правила сокрытия информации»;	(электронный ресурс).

Методическая разработка web-квеста по дисциплине «Информационная безопасность для экономистов» представлена в Приложении 5.

Применяя в работе со студентами квест-технологию, наблюдается положительная тенденция. Повышается эффективность обратной связи между студентами, изучаемой дисциплиной и преподавателем; стимулируется познавательная деятельность студентов;

возбуждается интерес к процессу обучения в целом. Технология Web-квест позволяет увеличивать эффективность педагогического процесса, формировать компетенции в области коммуникаций, саморазвития. Квест ставит перед обучающимися проблемную ситуацию, заставляет осуществить поиск и отбор информации. Web -квест положительно воздействует на учебную деятельность и способствует формированию у обучаемых информационно-коммуникативной компетенции, навыков работы в группе, самостоятельности, способности выделить оптимальный вариант и обосновать решение, опыт публичных выступлений.

С проектной деятельностью студентов неразрывно связана самостоятельная работа обучающихся, которая: 1) способствует личностно-ориентированной направленности будущих специалистов; 2) придает учебному процессу проблемно-исследовательский характер; 3) обеспечивает «саморазвитие необходимых способностей …к более сложным видам деятельности, способы и содержание которой не могут передаваться или осваиваться по образцам»; 4) формирует развитие ответственности за результаты своей деятельности, учебного процесса в целом[131, с. 330].

2.3.3 Методические аспекты балльно-рейтинговой системы оценивания

Для объективного оценивания результатов прохождения курса и для стимулирования работы студентов в течение семестра применяется *накопительная балльно-рейтинговая система,* с заранее определенными четкими границами и критериями. В самом начале изучения дисциплины студенты знакомятся с правилами, которые неизменны в течение семестра (табл. 2.3).

Таблица 2.3. Структура балльно-рейтинговой системы дисциплины

Баллы, которые студент может набрать в течение семестра	Рейтинг студента
10 баллов – активность в образовательном процессе; 40 баллов – практические работы; 10 – подготовка мультимедийной демонстрации на выбранную тему; 10 –участие в образовательном проекте; 30 баллов – промежуточная аттестация.	– «отлично» необходимо набрать более 90 баллов в течение семестра. – «хорошо» – от 75 до 89 баллов; – «удовлетворительно» – от 60 до 74 баллов; – «неудовлетворительно» – от 30 до 59 баллов; – «не допуск к промежуточной аттестации» менее 30 баллов.

Максимальный рейтинг студент может получить за работу в течение семестра (70 баллов) и при промежуточной аттестации, выполняемой в виде итогового тестирования (30 баллов). Наибольшее количество баллов студент набирает, успешно выполняя практические работы, изложенные в методических указаниях, размещенных в системе

[131] ТРЕТЬЯКОВА, Е. М. Организация самостоятельной работы студентов с применением новых информационных технологий. В: *Балтийский гуманитарный журнал*. 2016, Т. 5. № 4(17), с.329-333. ISSN 2311-0066.

дистанционного обучения. Их выполнение активизирует учебно-познавательную деятельность, улучшая процесс взаимодействия студента с окружающей действительностью, результатом которого является овладение знаниями на уровне воспроизведения или творчества, умениями и навыками, необходимых будущему специалисту[132].

При оценивании практических работ учитываются следующие моменты. Студент должен понимать содержание выполненной работы (знать определения понятий, описать значение и смысл терминов, используемых в работе и т.п.). Студент имеет право на доработку работы (по указаниям преподавателя) сроком не более недели без снижения балла. За несвоевременную сдачу практической работы исходный балл снижается на 10% за каждую неделю. Общий балл за практическую работу складывается из баллов, полученных с учетом просрочек и исправлений. Правильность выполнения работы оценивается в баллах в соответствии с таблицей 2.4.

Таблица 2.4. Критерии оценивания практических работ

Балл	Содержательная характеристика
1	В полностью выполненной работе отсутствует теоретический материал
2	В полностью выполненной работе практически не освещен теоретический материал, допущены ошибки по сущности рассматриваемых вопросов
3	В полностью выполненной работе теоретический материал изложен на минимально допустимом уровне.
4	В полностью выполненной работе отсутствуют теоретические ошибки но не сформулированы собственные, самостоятельные, обоснованные, аргументированные суждения студента.
5	В полностью выполненной работе отсутствуют теоретические ошибки, сформулированы собственные, самостоятельные, обоснованные, аргументированные суждения студента.

Текущее тестирование применяется в качестве *обучающего контроля* по пройденному теоретическому материалу, и баллами не оценивается. Текущее компьютерное тестирование помогает бороться с неравномерной работой студентов в семестре – отвечать на задания студентам становится полезно и интересно. В конце концов, они начинают интересоваться правильными ответами и, иногда, начинают по-иному рассматривать поставленные перед ними задачи. Поэтому текущее компьютерное тестирование можно рассматривать как стимул к самостоятельной работе.

При классической схеме образования преподаватель обучает студента, а потом экзаменует его. Хороший результат свидетельствует о том, что студент достаточно времени посвятил самостоятельной работе. При схеме, использующей текущее компьютерное тестирование, на студента воздействует не только полученный материал,

---

[132] МЕШКОВА, Л. М. Сущность и структурно-содержательные компоненты активизации учебно-познавательной деятельности студентов технических вузов. В: *Вестник Челябинского государственного педагогического университета,* 2010, №, с.119-125.

но и сам контроль знаний. Иными словами текущее компьютерное тестирование – это не только результат, но и инструмент для получения знаний (рис. 2.10).

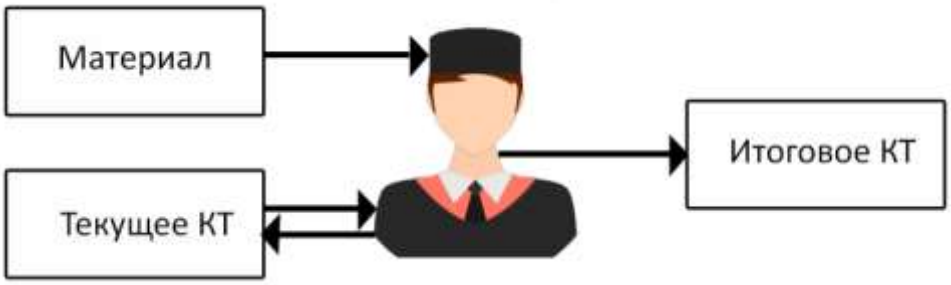


Рис. 2.10. Процесс обучения при использовании компьютерного тестирования

Такого плана текущий тест состоит из 3-4 вопросов и его прохождение занимает 3-5 минут. В конце изучения дисциплины проводится итоговое тестирование. Вопросы разработаны таким образом, чтобы охватить все темы дисциплины. Выделены разные уровни сложности (Приложение 6).

Тем не менее, компьютерное тестирование не должно полностью исключать другие методы оценивания, особенно для студентов очной формы обучения. Наоборот, его комбинация с классическими методами контроля позволяет получить студентам, и объективную оценку, и высокий уровень знаний и умений по дисциплине.

2.3.4 Междисциплинарные связи при изучении информационной безопасности

При реализации междисциплинарных связей необходимо придерживаться следующего ряда условий:

- организация самостоятельной работы с использованием информационных технологий;

- применение проектного метода обучения;

- использование комплекса задач и заданий, затрагивающих другие дисциплины.

Междисциплинарность заключается в решении сразу нескольких проблем. Так с математикой студенты соприкасаются при изучении способов парольной защиты и криптографии; с историей – при изучении криптографии; с психологией и социологией – при освещении вопросов организационной защиты информации; с экономикой – в разделе электронная цифровая подпись и алгоритмы хеширования и т.д. Такое взаимопроникновение наук позволяет повысить качество обучения, обосновать адекватность получаемых знаний реальной жизни.

На занятиях по информационной безопасности необходимо изучать нормы права, рассматривать исторические примеры, оперировать математическими и физическими понятиями, приводить примеры из литературы, принимать во внимание психологические и социологические аспекты. Связь отдельных тем курса с другими предметами

отображена в матрице межпредметных связей (табл. 2.5).

Таблица 2.5. Матрица межпредметных связей дисциплины «Информационная безопасность»

Тема дисциплины ИБ	экономика	математика	физика	география	история	литература	право	социология	психология
Т1	•						•		
Т2	•		•				•	•	•
Т3	•			•	•		•		•
Т4	•						•	•	•
Т5	•	•	•				•		
Т6	•	•					•		
Т7	•	•	•			•	•		•
Т8	•	•	•		•	•	•	•	•
Т9	•			•	•	•	•	•	•

Анализ таблицы 2.2 позволяет сделать вывод, что межпредметные связи прослеживаются на каждом занятии при изучении информационной безопасности. На уровне ознакомления, запоминания и понимания преподаются темы с наименьшим количеством связей. Особое внимание необходимо уделять правовым, морально-этическим способам защиты информации. Юридическая грамотность, морально-психологическая устойчивость к негативному информационному воздействию необходимы в профессиональной деятельности будущего экономиста.

Раздел «Криптографические подходы к защите информации и электронно-цифровая подпись» наряду с повышением уровня цифровой грамотности, способствует развитию математической компетенции[133], [134]. Студенты экономического профиля подготовки знакомятся с историей криптографии и классификацией современных алгоритмов в области защиты информации. Для них важнее понимание сущности электронно-цифровой подписи и получение навыков ее создания. Методическая разработка занятия по созданию и проверке подлинности подписи Эль-Гамаля представлена в публикации [135].

Особенно для студентов экономического профиля подготовки важно подчеркивать связь информационной безопасности с экономической. Каждый раздел дисциплины имеет

[133] BOGDANOVA, V., CHIRIAC, L. Repere didactice privind studierea algoritmilor care țin de autentificare și semnăturile digitale In: *Conferința Republicană a cadrelor didactice*, 1-2 martie 2019. Chișinău: UST, 2019. p.174-179.

[134] CHIRIAC, L, DANILOV, A., BOGDANOVA, V. Utilizarea conceptelor din teoria numerelor in elaborarea algoritmilor criptografici asimetrici In: *Învăţământ superior: tradiţii, valori, perspective, Conferinţa ştiinţifica naţionala cu participare internaţională*, 29-30 septembrie 2020. Chişinău: UST, 2020, p.239-247.

[135] БОГДАНОВА, В.А., КИРИЯК, Л. Л. Проектирование практического занятия по теме «Алгоритмы хеширования и электронно-цифровой подписи» для студентов гуманитарного профиля. In: *Învăţământ superior: tradiţii, valori, perspective, Conferinţa ştiinţifica naţionala cu participare international*, 28-29 septembrie 2018 года, Кишинэу: UST Printing, 2018, с. 134-138.

экономический подтекст (табл. 2.6).

Таблица. 2.6. Соотношение тем дисциплины «Информационная безопасность» с экономическими процессами

Тема дисциплины ИБ	Экономическая модель	Формируемая компетенция
Основные понятия защиты информации	Режим секретности; профессиональные тайны: банковская, коммерческая	ОПК-1
Угрозы ИБ и каналы утечки	Все информационные угрозы предприятия сводятся к экономическим рискам	ОПК-1, -4
Средства защиты информации	Ущерб от реализации информационных рисков	ОПК-1
Правовые и морально-этические нормы ИБ	Закон об авторском праве, типы лицензий на программное обеспечение	ОПК-1, 4
Организационные	Социальная инженерия	ОПК-1, 4
Программные	Ущерб от вредоносных программ: программ-шпионов, спама, вирусов, трояна и т.п.	ОПК-1 -3
Идентификация и аутентификация	Предотвращение несанкционированного доступа к информационным ресурсам и сервисам	ОПК-1 -3
Криптография	Электронный документооборот и электронно-цифровая подпись	ОПК-1 -3

Применение знаний из других предметов, оценка их значимости для будущей профессиональной деятельности способствует выработке новых обобщённых умений, формированию научного и идейно-нравственного мировоззрения. Овладение навыками на основе междисциплинарных связей, влияет на мотивационную сферу, успехи в учебной и трудовой деятельности.

Студентам экономических специальностей показывается последовательность возникновения таких явлений в профессиональной деятельности как информационные угрозы, информационные и экономические риски, экономический ущерб.

2.4 Выводы к главе 2

Развитие информационных и коммуникационных технологий жизненно важно для конкурентоспособности Республики Молдова в сфере экономике, которая стремительно становится все более цифровой. Инновации с применением передовых ИКТ становятся движущей силой социально-экономических изменений, включая переосмысление образовательной парадигмы. Таким образом, проанализированы предоставляемые ИКТ преимущества и аргументирована полезность их внедрения в образовательное пространство вуза. В частности, рассмотрен процесс повышения качества изучения технологий защиты информации и информационной безопасности с позиции интернет-технологий в профессиональной подготовке студентов финансово-экономической сферы.

Для реализации этого процесса были разработаны и внедрены активные методологии обучения, сосредоточенные на учащемся и ориентированные на

формирование у него компетенций и навыков к непрерывному обучению, посредством эффективного и дружественного сотрудничества педагог-студент в процессе преподавания-обучения-оценивания. В этом контексте можно выделить следующие результаты исследования:

1. Разработана педагогическая модель изучения технологий защиты информации будущими специалистами финансово-экономической сферы посредством интернет-технологий, что способствует расширению возможностей усвоения материала, росту самомотивации к непрерывному обучению и повышению эффективности процесса преподавание-учение-оценивание университетской дисциплины «Информационная безопасность». Преимуществом разработанной модели является учет междисциплинарных связей и учет корреляции между информационной и экономической безопасностью в формировании теоретических и практических направлений развития и совершенствования читаемой дисциплины.

2. Разработана и обоснована: теоретически и практически методология реализации предложенной модели путем применения интерактивных стратегий, основанных на современных подходах личностно-ориентированного обучения и направленных на развитие критического мышления.

3. Теоретически обосновано, что для эффективной реализация предложенной педагогической модели в процессе обучения дисциплине «Информационная безопасность» необходимо:

a) реализовывать содержание обучения в организационных формах, способствующих проявлению познавательной активности и профессиональной направленности студентов, таких как лекции-дискуссии, лекции-конференции, видеолекции, тематическая, групповая дискуссии;

b) организовывать самостоятельную внеаудиторную деятельность студентов: проектную деятельность, веб-квест, «устранение цифрового неравенства»;

c) применять такие методы мотивации и стимулирования учебно-познавательной деятельности как: балльно-рейтинговая система, подготовка презентаций студентами, участие в студенческих конференциях;

d) использовать технологии обучения, способствующие повышению уровня обученности студентов в процессе изучения дисциплине «Информационная безопасность» и расширению опыта использования полученных умений и навыков в личной жизни и будущей профессиональной деятельности;

e) для формирования практических навыков использовать лабораторные работы по программным способам защиты информации, с применением различных средств, а также

использовать встроенные утилиты операционных систем, современное свободно распространяемое программное обеспечение, такое как drweb Cureit, cCleaner, 7-Zip;

f) применять он-лайн инструменты в процессе преподавания-обучения-оценивания, такие как Joomag, TestMoz, GoogleSites, GoogleForms, необходимые для оперативного представления, при необходимости изменения учебно-методических материалов для организации учебного процесса в стенах образовательного учреждения и за его пределами;

g) применять междисциплинарный подход, способствующий выработке новых обобщённых умений, формированию научного и идейно-нравственного мировоззрения; оказывающий влияние на мотивационную сферу, успехи в учебной и трудовой деятельности;

h) подчеркивать взаимосвязь информационной безопасности с экономической безопасностью, а также ее отражение на экономических процессах, для понимания значимости получаемых умений и навыков в совей будущей профессиональной деятельности.

4. Показано, что применение в дидактическом процессе разработанной педагогической модели интенсифицирует отношения сотрудничества и партнерства между студентом и преподавателем, способствует укреплению дружественной образовательной среды, благоприятствующей динамизации и эффективности учебного процесса

5. Полученные результаты дают возможность решить поставленную задачу исследования и достичь поставленных целей для повышения качества учебного процесса по рассматриваемой вузовской дисциплине и обеспечения результатов обучения за счет качественной интеграции информационно-коммуникационных технологий, в том числе интернет-технологий в учебный процесс.

3 ЭКСПЕРИМЕНТАЛЬНОЕ ОБОСНОВАНИЕ ЭФФЕКТИВНОСТИ ПЕДАГОГИЧЕСКОЙ МОДЕЛИ И МЕТОДОЛОГИИ ЕЁ ПРИМЕНЕНИЯ

3.1 Виды педагогических исследований

Методы научного познания в теории обучения

Исследовательских методов в педагогической науке существует множество. Они аналогичны методам и в других науках. В педагогике их применяют для решения конкретных педагогических задач. Педагогическое исследование – комплексный, многоаспектный процесс, вписанный в реальный процесс обучения, способствующий решению педагогических задач, благодаря единству исследовательской и практической учебно-воспитательной работы.

Научное педагогическое исследование – процесс формирования новых педагогических знаний, вид познавательной деятельности, направленный на открытие объективных закономерностей обучения, воспитания и развития [136, с.22].

При этом в педагогическом исследовании обязательно участвуют педагог и воспитанник, функционируют и развиваются педагогические отношения, решаются педагогические задачи. Педагогическое исследование требует осторожного взвешенного подхода к нововведениям, чтобы минимизировать степень возможного риска, не навредить детям, воспитанникам [137 , с.49].

Методы исследования, применяемые в педагогике, являются общими для ряда наук. Эти методы часто называют общенаучными логическими методами познания.

Различают три уровня педагогических исследований:

– эмпирический – на основе опыта, практики, экспериментов устанавливаются новые факты в педагогической науке;

– теоретический – абстрагируясь от реальности, строятся модели, выдвигаются и формулируются основные, общие педагогические закономерности, позволяющие объяснить раннее открытые факты и предсказать их будущее развитие;

– методологический – на базе эмпирических и теоретических исследований формулируются общие принципы и методы исследования педагогических явлений,

---

[136] ФЕДОТОВА, Г. А. *Методология и методика психолого-педагогических исследований*. Великий Новгород: НовГУ, 2010. 114 с.

[137] ЗАГВЯЗИНСКИЙ, В. И., АТАХАНОВ, Р. *Методология и методы психолого-педагогического исследования*. 2-е изд. Москва: Издательский центр «Академия», 2005. 208 с. ISBN 5-7695-2146-5.

построения теории [там же, с. 90; 138 с.22].

В настоящее время в теории обучения особенно популярны эмпирические методы научного познания (наблюдение, самонаблюдение, беседа, интервью, анкетирование, эксперимент, анализ продуктов деятельности (творчества), тестирование)[139]. В педагогическом эксперименте заинтересованы педагогическое сообщество, государство, учащиеся и их родители (рис. 3.1.).

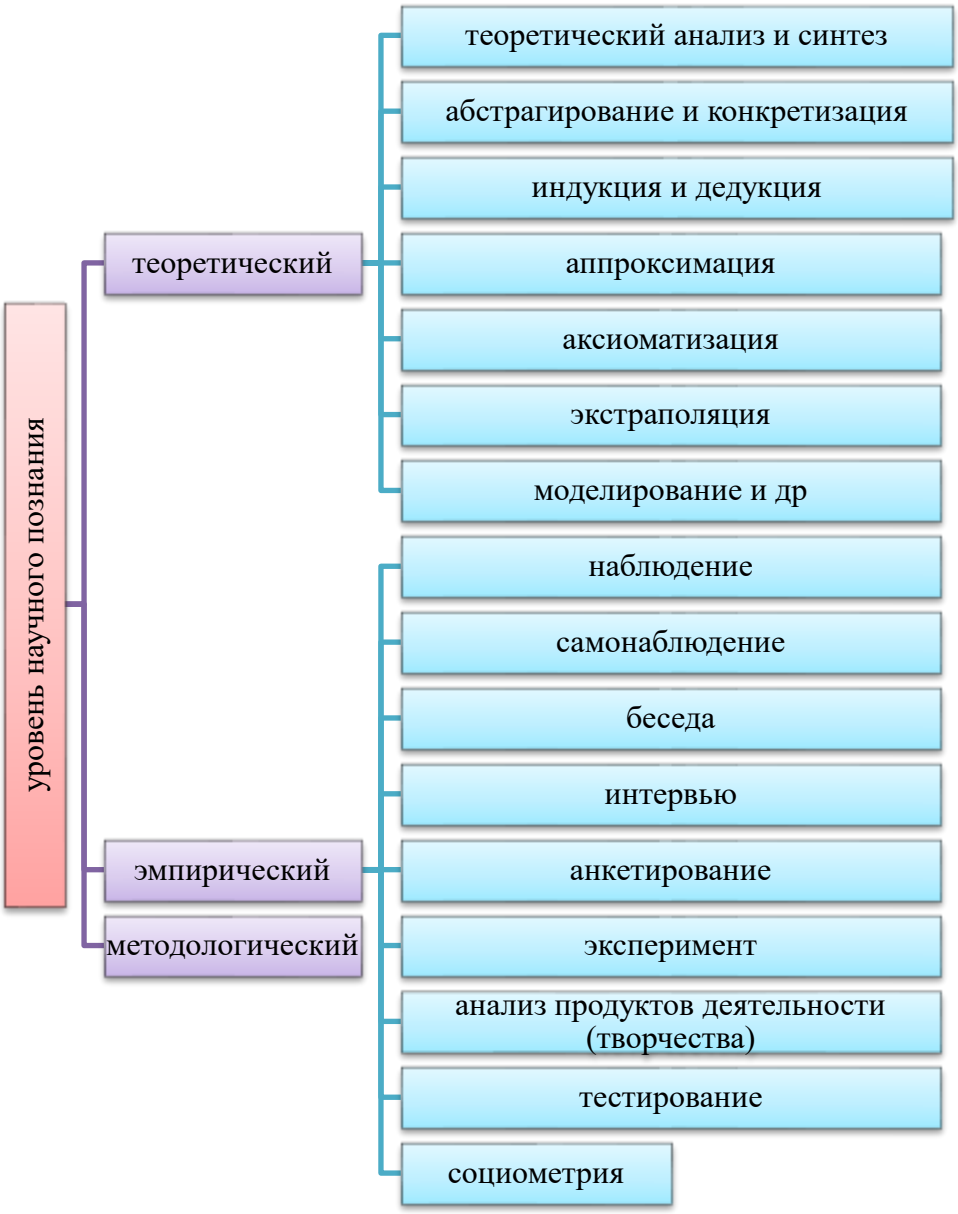


Рис. 3.1. Уровни научного познания

Сущность и содержание понятия «педагогический эксперимент»

На сегодняшний день существуют разные определения термина *эксперимент*.

В «**Большом толковом словаре официальных терминов: Более 8000**

[138] ФЕДОТОВА, Г. А. *Методология и методика психолого-педагогических исследований*. Великий Новгород: НовГУ, 2010. 114 с.
[139] ЗИМНЯЯ, И. А. *Педагогическая психология*. 2-е изд. Москва: Логос, 2001. 208 с. ISBN 5-88439-097-1.

терминов», составленным Ю. И. Фединским, на основе терминов, взятых из законодательных и нормативных и документов, эксперимент – это «система операций, воздействий и/или наблюдений, осуществляемых при выполнении исследовательских работ и направленных на получение информации об объекте»[140, с.981].

В словаре **Ожегова** эксперимент, то же что опыт, либо попытка сделать, предпринять что-нибудь[141, с. 908]. Опыт же – это «воспроизведение какого-нибудь явления экспериментальным путем, создание чего-нибудь нового в определенных условиях с целью исследования, испытания.

В **педагогическом энциклопедическом словаре** под ред. Б. М. Бид-Бад педагогический и психологический *эксперимент* (от лат. experimentum - опыт, проба) является «одним из основных (наряду с наблюдением) методов научного познания». В контролируемых и управляемых условиях исследователь изучает явления действительности для выявления изменений в поведении человека при планомерном манипулировании определяющими это поведение факторами (переменными) [142].

В «**Краткой философской энциклопедии**» эксперимент определяется как «планомерно проведенное наблюдение; планомерная изоляция, комбинация и варьирование условий с целью изучения зависящих от них явлений» [143, с.535].

В начале 20 века немецкие ученые В. А. Лай и Э. Мёйманом начали активно разрабатывать экспериментальную педагогику. В. А. Лай считал, что экспериментальный метод в педагогике и полученные с его помощью результаты дополнит и расширит, обогатит классическую педагогику, является ее логическим развитием. Методами экспериментальной педагогики и дидактики являются «самонаблюдения и наблюдения за посторонним лицом, статистические наблюдения (статистику) и экспериментальные наблюдения (эксперименты)» [цит. по 144, с.129]. Особенно выделяя гипотезу В. А. Лай определяет главные составляющие эксперимента: построение гипотезы, постановка и проведение опыта, проверка его на практике.

Важным В. А. Лай считал и то, что каждое педагогическое исследование должно основываться на общих, систематических точек зрения педагогики, иначе оно лишается

---

[140] ФЕДИНСКИЙ, Ю.И. *Большой толковый словарь официальных терминов: Более 8000 терминов*. Москва: ООО «Издательство Астрель»: ООО «Издательство АСТ, ООО «Транзиткнига», 2004. 1165 с. ISBN 5-17-020421-3.

[141] ОЖЕГОВ, С.И., ШВЕДОВА, Н. Ю. *Толковый русский словарь русского языка 80 000 слов и фразеологических выражений*. 4-е изд. Москва: ООО «А ТЕМП», 2006. 944 с. ISBN 978-5-9900358-6-7.

[142] БИМ-БАД, Б.М. М.М. *Педагогический энциклопедический словарь*. 3-е изд. Москва: Большая Российская энциклопедия, 2009. 527 с. ISBN 978-5-85270-230-2.

[143] ГУБСКИЙ, Е.Ф., КОРАБЛЕВА, Г.В., ЛУТЧЕНКО, В.А. *Краткая философская энциклопедия*. Москва: Прогресс - Энциклопедия, 1994. 576с. ISBN 5-01-004135-9.

[144] РОМАНОВ, А. А. Становление экспериментальной педагогики в Германии (к 150-летию со дня рождения В. А. Лая и Э. Мёймана). В: *Историко-педагогический журнал*. 2012, № 4. с. 122-138. ISSN 2304-1242.

педагогического характера.

В. А. Лай и Э. Мёйманом оказались провидцами. И в настоящее время невозможно представить себе педагогику без экспериментальных исследований.

В популярном американском учебнике по психологии **Ernest Hilgard** эксперимент определяется как наиболее эффективный научный метод, т.к. имеется возможность осуществлять точный контроль за переменными для выявления взаимосвязи между ними [145 p.31].

Sorin Cristea под педагогическим экспериментом, ценным в учебной деятельности, понимает дидактический / образовательный метод, в котором прямое исследование реальности происходит в конкретных условиях лаборатории, кабинета, школьной мастерской и т.д. Эксперимент направлен на формирование-развитие интеллектуального духа учащегося, с применением научных знаний в производственных контекстах [146].

Рассматривая педагогический эксперимент как вид педагогического исследования, всегда выделяют его основные этапы: поиск, обучение и проверка [147, с.19].

Теоретическими разработками в области методологии педагогического исследования занимались в разное время советские и российские ученые Г.В. Воробьев, В.И. Загвязинский, В. В. Краевский, А.М. Новиков, М. Н. Скаткин, М. М. Поташник, А.С. Сиденко и др.

Загвязинский В.И., определяет эксперимент как «исследовательский метод, который заключается в том, чтобы создать исследовательскую ситуацию, получить возможность ее изменять, варьировать ее условия, сделав возможным и доступным изучение психических процессов или педагогических явлений через их внешние проявления, раскрывая тем самым механизмы и тенденции возникновения и функционирования изучаемого явления» [148, с.108] .

Эксперимент в научной деятельности – это воспроизводимое средство соотношения теории и практики для проверки гипотез в педагогической деятельности. Эксперимент служит для доказательности результатов исследования [**В.В. Краевский**, с.41, 150,160][149].

---

[145] АТКИНСОН, Р. Л., АТКИНСОН, Р. С., СМИТ, Э. Е., БЕМ, Д. Дж. *Введение в психологию*. 13 изд. 2003. 713 с. ISBN 5-93878-097-7.

[146] CRISTEA, S. *Dictionar de Termeni Pedagogici*. Bucureşti: Editura didactică şl pedagogică, 1998. 312 p. ISBN 973-30-5130-6.

[147] SILISTRARU, Nicolae. GOLUBIŢCHI, Silvia *Pedagogia învăţământului superior: Ghid metodologic.* Chişinău: UST, 2013. 192 p. ISBN 978-9975-76-102-4.

[148] ЗАГВЯЗИНСКИЙ, В. И., АТАХАНОВ, Р. *Методология и методы психолого-педагогического исследования.* 2-е изд. Москва: Издательский центр «Академия», 2005. 208 с. ISBN 5-7695-2146-5.

[149] КРАЕВСКИЙ, В. В. *Методология педагогического исследования*. Самара: СамГПИ. 1994. 165 с. ISBN 5-8428-0038-1.

Академик **Бабанский Ю.К**. в труде «Проблемы повышения эффективности педагогических исследований» писал, что «эксперимент позволяет обнаружить повторяющиеся, устойчивые, необходимые, существенные связи между явлениями, т. е. изучать закономерности, характерные для педагогического процесса»[150 с.73] . Психолого-педагогический эксперимент – комплексный метод исследования, который обеспечивает научно-объективную и доказательную проверку правильности обоснованной в начале исследования гипотезы. Он позволяет проверить эффективность тех или иных нововведений в области обучения и воспитания, сравнить значимость различных факторов в структуре педагогического процесса и выбрать наилучшее (оптимальное) для соответствующих ситуаций их сочетание, выявить необходимые условия реализации определенных педагогических задач.

Зимняя А.И. определяет эксперимент как «центральный эмпирический метод научного исследования, получивший широкое распространение в педагогической психологии… В его ходе изучаются изменения в уровне знаний, умений, отношений, ценностей, в уровне психического и личностного развития обучающихся под целенаправленным обучающим и воспитывающим воздействием»[151, с.15].

Сиденко А.С. в своих исследованиях делает акцент на возможности воспроизвести эксперимент, проверить гипотезу, установить и уточнить факты. «Эксперимент – это исследовательская деятельность, предназначенная для проверки выдвинутой гипотезы, разворачиваемая в естественных или искусственно созданных контролируемых и управляемых условиях, результатом которой является новое знание, включающее в себя выделение существенных факторов, влияющих на результаты педагогической деятельности» [152, с.22].

Поляков В.П. говорит о сущности педагогического эксперимента: «*исследовательская деятельность экспериментатора включает фиксацию значений переменных, в которых описывается изучаемая причинно-следственная закономерность, и организацию экспериментальных воздействий посредством управления условиями, выступающими в качестве независимых переменных. Решение вопроса о том, что наблюдать и измерять, а также какие формы контроля экспериментальных воздействий организовывать определяется системой гипотез как регуляторов и ориентиров*

[150] ФЕДОТОВА, Г.А. *Методология и методика психолого-педагогических исследований*. Великий Новгород: НовГУ. 2010. 114 с.
[151] ЗИМНЯЯ, И. А. *Педагогическая психология*. 2-е изд. Москва: Логос, 2001. 208 с. ISBN 5-88439-097-1.
[152] СИДЕНКО, А.С., ХМЕЛЕВА, В. С. Педагогический эксперимент: понятие и этапы деятельности. В: *Эксперимент и инновации в школе*. 2008, №2, с.21-25.

практической деятельности экспериментатора» [153, с.373] .

Определение педагогического эксперимента, сформулированное Поляковым В. П., видится в нотациях кибернетического подхода, так как речь идет об управлении сложной системой с получением обратной связи, но при этом экспериментатор не всегда может контролировать некие внутренние элементы системы. Можно сказать, что педагогический эксперимент является своего рода черным ящиком, для которого известен вход, запланирована цель (выход), но что внутри не ясно.

Виды экспериментов в педагогических исследованиях

В педагогических исследованиях принято проводить сначала констатирующий, или зондирующий эксперимент, затем уточняющий, на финальном этапе исследования формирующий, или созидательно-преобразующий.

На основе работ Загвязинского В. И., Краевского Г. В., Новикова А. М., Скаткина М. Н., Поташника М. М., Сиденко А. С., Зимняя И. А., Федотовой и др. составлена схема классификаций педагогического эксперимента (рис. 3.2).

Зондирующий, или как его иногда называют разведывательный эксперимент, проводится на подготовительном этапе с ограниченным составом учащихся для повышения качества исследования: оценка правильности построения программы эксперимента, внесение корректив. Такой эксперимент может быть как краткосрочным, так и долгосрочным.

Констатирующий эксперимент состоит в констатации фактов о наличии причинно-следственных связей, зависимости между явлениями, таким образом исследователь изучает состояние изучаемой педагогической системы.

Уточняющий (проверочный) эксперимент позволяет проверить выдвинутую гипотезу исследования.

Формирующий эксперимент – активное воздействие исследователя на изучаемую систему, и направлен на формирование у испытуемых определенных качеств, повышение результативности учебной и трудовой деятельности.

[153] ПОЛЯКОВ, В. П. *Методическая система обучения информационной безопасности студентов вузов*: дис. ... д-ра пед. наук. Н. Новгород, 2006. 538 с.

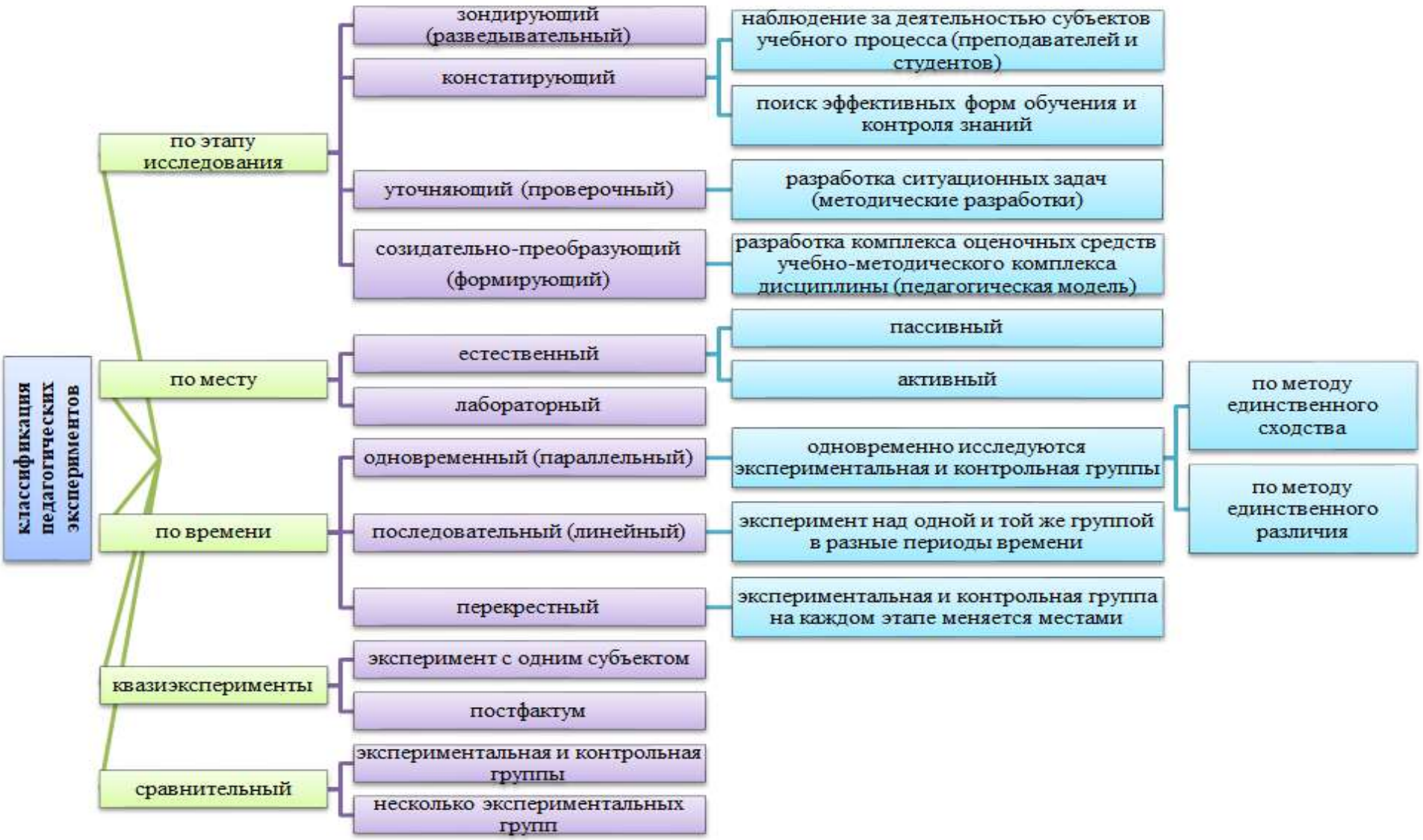


Рис. 3.2. Виды экспериментов в педагогике

Лабораторный эксперимент, подразумевает создание искусственных условий для моделирования некоторой части естественной деятельности. Лабораторный эксперимент является моделью реальной ситуации, но не учитывает все факторы и воздействия, а только те, которые интересуют исследователя. Испытуемый находится в определенных условиях, знает о том, что является участником эксперимента, но не знает о его целях. Лабораторные эксперименты в педагогике и психологии начали проводить в XIX веке. Примерами являлись в разное время педагогические лаборатории немецкого исследователя педагога В.А. Лая, опытные станции С.Т. Шацкого в 20-х годах XX века в СССР.

По сути, искусственность лабораторной ситуации является сильной стороной, но также и наиболее уязвимой. С одной стороны, благодаря лучшему контролю внешних переменных и возможности изучения сложных переменных, можно однозначно определить причинно-следственные связи, с другой стороны, абстракция переменных от их естественного контекста, их комбинация в соответствии с экспериментальной моделью является искажением их действия.

Экспериментатор выбирает наиболее значимые со своей точки зрения характеристики для изучения, таким образом, не все факторы входят в эксперимент. Экспериментатор предполагает, какой результат он собирается получить, и может непреднамеренно провоцировать испытуемых, которые в свою очередь могут реагировать соответствующим образом для получения вознаграждения и т.п.

Естественный эксперимент был применен и предложен в педагогической практике А.Ф. Лазурским в 1910 г. [цит. по кн. Загвязинский В.И., с.110]. В отличие от лабораторного, естественный проводится в привычных для испытуемых условиях деятельности, с созданием или воссозданием явления, которое изучает исследователь. Появляется возможность замаскировать от испытуемых содержание и цели эксперимента. Этот тип эксперимента, дополняющий лабораторный, имеет в целом те же характеристики: порождение явления путем изменения условий, его повторение и т. д.

Преимущества естественного эксперимента многочисленны:

– субъекты наблюдаются в естественных условиях;

– независимые факторы не исключаются;

– экспериментатор не оказывает своего непосредственного влияния на экспериментальную ситуацию;

– мотивация учащихся генерируется реальной ситуацией, а не созданной (ожидаемой наградой), что может служить основой для более обоснованных выводов.

По этой причине естественный эксперимент находит большую область применения

в образовании: внедрение новых учебных методик, оценка результатов деятельности учащихся, изменение рабочих программ и т.п. Все это совершенствует учебно-воспитательный процесс.

Преимущества с одной стороны (естественные пути развития, реализм, соответствие внешней среде) достигаются ценой некоторых недостатков:

– в естественном эксперименте присутствует целый ряд возмущающих факторов (внешних и внутренних);

– строгий контроль переменных намного сложнее, чем в лабораторном эксперименте;

– экспериментатор не всегда готов к реальной ситуации;

– многие ситуации необратимы, поэтому вероятность их создания или повторения очень мала;

– реальная ситуация затрудняет выбор и сопоставление объясняющих переменных, осложняет определение причинно-следственных связей.

В естественном исследовании различают пассивную и активную модель.

Пассивный естественный эксперимент предполагает, что исследователь не манипулирует условиями, не проводит экспериментальные воздействия, а наблюдает, и ищет причинно-следственные связи, возникающие в ходе эксперимента.

Активный естественный эксперимент предполагает, что исследователь прямо или косвенно осуществляет экспериментальное воздействие на испытуемых.

По времени проведения выделяют одновременный и последовательный эксперименты. Одновременный – подразумевает проведение эксперимента над экспериментальной группой и одновременное сравнение ее с контрольной группой. Последовательный – сравнение во времени изменений происходящих в результате экспериментального воздействия над экспериментальной группой обучающихся.

Последовательный (линейный) эксперимент. В его основе лежит сравнение объекта с самим собой, но в разные периоды времени. В педагогике на разных этапах обучения. Сначала измеряется интересующий исследователя параметр – констатирующий замер. Затем проводится эксперимент без изменения содержания, методов и средств обучения. Осуществляется контрольный замер. На следующем этапе в группе испытуемых проводится эксперимент с нововведениями и вновь осуществляется контрольное измерение интересующего параметра. Если во втором случае результат выше, чем в первом, то делается вывод о положительном влиянии исследовательского нововведения.

Одновременный (параллельный) эксперимент. В его основе лежит сравнение нескольких объектов между собой. Обычно сравнивают контрольную и

экспериментальную группу. В экспериментальной группе в учебный процесс вносится нововведение. В контрольной обучение происходит по традиционной методике, либо с использованием новых средств обучения. Осуществляется контрольное измерение, и если результат в экспериментальной группе по изучаемому параметру выше, чем в контрольной группе, то делается вывод о положительном влиянии экспериментального воздействия на педагогический процесс.

Параллельный эксперимент может проводиться по двум схемам: сравнение по методу единственного сходства и по методу единственного различия.

В параллельном эксперименте по методу единственного сходства экспериментальными являются несколько групп, которые подвергаются проверяемому воздействию фактора Ф. Однако, кроме фактора Ф, одинакового для всех групп, в педагогическом процессе действуют другие скрытые и не учитываемые факторы: влияние личности учителей, методы обучения, особенности групп и др. Если в таких условиях в результате эксперимента будет зарегистрировано одно и то же одинаковое для всех объектов изменение исследуемого параметра, то это должно являться следствием воздействия фактора Ф.

Параллельный эксперимент по методу единственного различия предполагает уравнивание всех факторов обучения в двух группах объектов, поэтому реализовать его несколько труднее. Затем в одной группе (экспериментальной) проводится испытуемое воздействие, а в другой (контрольной) процесс идет без такого воздействия. Если оказывается, что в экспериментальной группе результаты обучения, или воспитания выше, чем в контрольной (единственное различие), то это считается следствием применения испытуемого воздействия.

Перекрестный эксперимент проводится в случае, когда уравнять учащихся и все условия в контрольной и экспериментальной группах нет возможности. Выход из этого положения состоит в том, что контрольные и экспериментальные группы меняются местами в каждой последующей серии экспериментов. Сначала осуществляется формирующее воздействие на объект А, проводится контролирующий эксперимент. Затем осуществляется формирующее воздействие на объект Б, проводится контролирующий эксперимент. Если обнаруживается повышение уровня знаний в экспериментальной группе в каждом случае, то говорят о вполне надежном эффекте от применяемого исследователем нововведения.

Эксперимент *ex post facto* впервые ввел Chapin, Qeen. Исследователи такой тип эксперимента относят к квазиэкспериментальным исследованиям, т.е. к таким исследования в которых нет возможности сделать выводы о причинно-следственных

связях из-за неполного контроля над переменными. Экспериментальное исследование по типу ex post facto происходит после того как событие уже произошло. Таким образом экспериментатор не воздействует на испытуемых, а анализирует произошедшие реальные события. Суть такого эксперимента состоит в попарном уравнивании состава группы на основании сведений об испытуемых

Сравнительный эксперимент подразумевает сравнение объектов. Это может быть сравнение экспериментальной и контрольной групп обучающихся, либо сравнение нескольких экспериментальных групп между собой для выявления наилучшего результата. В экспериментальной группе, как правило, организуются специальные педагогические изменения, которые должны привести к позитивным результатам.

Экспериментальные планы

Планирование эксперимента помогает спроектировать оптимальную последовательность действий (модель), тем самым добиваясь валидности, надёжности и точности результатов исследовании. Классификацию экспериментальных планов с точки зрения близости к идеальному дана Donald T. Cambell. Он делит их на: доэкспериментальные (*three preexperimental designs*), планы истинных экспериментов (*three true experimental designs*) и квазиэкспериментальные планы (*quasi-experimental designs*) [154]. Систематизированные признаки доэкспериментальных, квазиэкспериментальных планов и планов истинных экспериментов приводятся в нижеследующей таблице 3.1 [155].

Таблица 3.1. Классификация экспериментальных планов данная Donald T. Campbell

Доэкспериментальные планы	Планы истинных экспериментов	Квазиэкспериментальные планы
Неэквивалентность групп или отсутствие контрольной группы. Отсутствие или низкие возможности контроля угроз валидности. Наличие значительного количества угроз внутренней валидности и отсутствие внешнего контроля. Невозможность вывода об однозначной каузальной связи	Наличие стратегии формирования эквивалентных экспериментальных групп (рандомизации). Наличие двух или более экспериментальных групп. Возможность вывода об однозначной казуальной связи. Широкие возможности контроля переменных. Завершение эксперимента измерение и сравнением результатов в разных группах.	Проведение эксперимента в естественных условиях, при трудностях контроля. Наличие контрольной группы или серии измерений эффекта экспериментального воздействия. Возможность сравнения результатов экспериментальных групп или результатов одной группы до и после экспериментального воздействия. Ограниченные возможности управления переменными.

[154] КЭМПБЕЛЛ, Д. *Модели экспериментов в социальной психологии и прикладных исследованиях*. Москва: Прогресс, 1980. 390 с.
[155] ГОРБУНОВА, В.В. *Экспериментальная психология в схемах и таблицах*. Киев: ВД «Професіонал, 208 с. ISBN 978-966-370-067-0.

Доэкспериментальные планы менее всего учитывают требования, предъявляемые к идеальному эксперименту. В.Н. Дружинин указывает, что они могут служить лишь иллюстрацией, в практике научных исследований их следует по возможности избегать [156].

Квазиэкспериментальные планы являются попыткой учета реалий жизни при проведении эмпирических исследований, они специально создаются с отступлением от схем истинных экспериментов. Исследователь осознает, что есть внешние факторы, которые он не может контролировать. Квазиэкспериментальный план применяется тогда, когда применение лучшего плана невозможно.

3.2 Краткая характеристика педагогического исследования

3.2.1 Проектирование педагогического эксперимента с позиции системного подхода

Научное педагогическое исследование – процесс формирования новых педагогических знаний, вид познавательной деятельности, направленный на открытие объективных закономерностей обучения, воспитания и развития [157, с. 2]. Рассматривая педагогический эксперимент, как вид педагогического исследования, ученые Загвязинский В. И., Зимняя И. А., Сиденко А. С. и др., выделяют его основные этапы: зондирующий, констатирующий, уточняющий и формирующий[158, 159, 160]. Большинство педагогических экспериментов основаны на сравнении объектов: экспериментальной и контрольной групп обучающихся, нескольких экспериментальных групп между собой. В экспериментальной группе, как правило, организуются специальные педагогические изменения, которые должны привести к позитивным результатам.

Изучены педагогические исследования по обучению информационной безопасности студентов вуза, этапы и сущность педагогических экспериментов в диссертационных работах Полякова В. П. и Абиссовой М. А. (методики обучения студентов гуманитарного профиля подготовки), Боярова Е. Н. и Димова Е. Д. (дидактические приемы обучения студентов по направлению подготовки информационная безопасность и жизнедеятельность).

В проектировании педагогического эксперимента по обучению информационной

---

156 КОНОВАЛОВА, М.Д. *Экспериментальная психология: конспект лекций*. Москва: Высшее образование, 2009. 180 с. ISBN 5-9692-0082-4.

157 ФЕДОТОВА, Г.А. Методология и методика психолого-педагогических исследований. Великий Новгород: НовГУ. 2010. 114 с.

158 ЗАГВЯЗИНСКИЙ, В. И., АТАХАНОВ, Р. *Методология и методы психолого-педагогического исследования.* 2-е изд. Москва: Издательский центр «Академия», 2005. 208 с. ISBN 5-7695-2146-5.

159 ЗИМНЯЯ, И. А. Педагогическая психология. 2-е изд. Москва: Логос, 2001. 208 с. ISBN 5-88439-097-1.

160 СИДЕНКО, А.С., ХМЕЛЕВА, В. С. Педагогический эксперимент: понятие и этапы деятельности. В: Эксперимент и инновации в школе. 2008, №2, с.21-25.

безопасности будущих экономистов применен информационно-кибернетический подход, подразумевающий:

– анализ педагогической системы с точки зрения связей управления и информационных потоков, которыми обмениваются управляющая и управляемая подсистемы (педагог и обучающийся);

– оптимизацию процесса обучения, нахождение наиболее эффективных форм и методов организации учебного процесса, чтобы при наименьших затратах получить максимальный результат;

– практическое использование электронных устройств и автоматизированных обучающих систем для управления процессом обучения и тестирования; программированное обучение [161, с.3].

Системный подход лежит в основе процесса обучения в кибернетической педагогике [там же с.7]. При исследовании систем изучают структуру и взаимосвязи с помощью моделей: 1) «черный ящик»; 2) состав системы; 3) структуры системы.

При проектировании и реализации педагогического эксперимента по обучению информационной безопасности будущих экономистов использовали системный подход: на каждом этапе строили и анализировали одну из вышеперечисленных моделей:

1) поисковый этап → модель «черный ящик»;

2) констатирующий этап → модель состава системы;

3) уточняющий этап → модель структуры системы;

4) формирующий этап → оптимизация педагогической модели.

На первом, поисковом, этапе эксперимента процесс обучения рассмотрен с позиции модели «черный ящик», базирующейся на таких свойствах системы как «целостность» и «обособленность от среды». Система связана с внешней средой, имеет входы и выходы (цель) [162, с. 780].

В качестве входов служили существующие учебно-методические разработки по обучению информационной безопасности студентов технических специальностей, рабочие программы по дисциплине ведущих российских вузов, учебная литература по информационной безопасности, педагогические исследования по обучению информационной безопасности студентов гуманитарных направлений подготовки в вузе, освещенные в диссертационных работах Полякова В. П., Абиссовой М. А., Боярова Е. Н.,

---

[161] МАЙЕР, Р. В. *Кибернетическая педагогика: имитационное моделирование процесса обучения:* монография. Глазов: Глазов. гос. пед. ин-т, 2014. 141 с. ISBN 978-5-93008-176-3.

[162] ВОЛКОВА, В. Н., ЕМЕЛЬЯНОВ, А. А. и др. *Теория систем и системный анализ в управлении организациями: Справочник*. Москва: Финансы и статистика, 2006. 848 с. ISBN 5-279-02933-5.

Димова Е. Д. [163]и др.

В качестве цели обучения информационной безопасности будущих экономистов определена общепрофессиональная компетенция федерального государственного образовательного стандарта (ФГОС РФ) высшего образования по направлению подготовки 38.03.01 Экономика (уровень бакалавриата): «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности» (ОПК-1) [164].

На втором, констатирующем, этапе педагогического эксперимента, в рамках информационно-кибернетического подхода, построена модель состава системы.

В обучении информационной безопасности будущих экономистов выделили подсистемы: преподавание, учение, оценивание. Для каждой подсистемы проанализированы существующие решения, сформирован электронный учебно-методический комплекс (электронный конспект лекций, электронные методические указания к выполнению лабораторных работ, электронный тестовый комплекс). В дальнейшем происходила его оптимизация для достижения заданной цели.

На третьем, уточняющем, этапе педагогического эксперимента, в рамках информационно-кибернетического подхода, построена модель структуры системы. Иногда для описания системы недостаточно моделей «черный ящик» и «состава системы». В первом случае описывается окружение изучаемой системы, во втором – подсистемы и элементы. При построении модели обучения информационной безопасности будущих экономистов необходимо учесть взаимосвязи между подсистемами и элементами. Синтез выбранных подсистем и элементов, отражение их взаимосвязи позволяет построить оптимальную модель обучения информационной безопасности будущих экономистов. В итоге построена педагогическая модель.

На четвертом, формирующем, этапе педагогического эксперимента, в рамках информационно-кибернетического подхода проверялась эффективность построенной педагогической модели обучения.

Краткая характеристика педагогического эксперимента по обучению основам защиты информации и информационной безопасности будущих специалистов финансово-экономической сферы представлена в таблице 3.2.

---

[163] ДИМОВ, Е. Д. *Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования*, дис. канд. пед. наук. Москва, 2013. 181с.

[164] *ФГОС ВО по направлениям бакалавриата*. Портал Федеральных государственных образовательных стандартов высшего образования РФ, ©2021 [citat 04.07.2021]. Доступен: https://fgosvo.ru/fgosvo/index/4/88.

Таблица 3.2. Краткая характеристика педагогического эксперимента

№	Этапы педагогического эксперимента	Годы	Количество человек	Метод исследования	Краткое описание
1	поисковый	2014-2015	57	Анализ и синтез, анкетирование, моделирование	Анализ текущего состояния
2	констатирующий	2015-2017	74	Анализ деятельности, тестирование	Формирование дидактической системы
3	уточняющий	2017-2018 2018-2019	56 31	эксперимент	Оптимизация дидактической системы
4	формирующий	2019-2020 2020-2021	35 20	эксперимент	Проверка эффективности разработанной дидактической системы
	Итого, чел.		273		

3.2.2 Поисковый эксперимент

Поисковый этап педагогического эксперимента реализовывался в 2014-2015 гг. с целью формулирования результатов обучения технологиям защиты информации будущих экономистов, исследовании стандартов, учебно-методической и научной литературы в области информационной безопасности, а также требований рынка.

При рассмотрении проблем, связанных с обучением информационной безопасности студентов экономического профиля подготовки были проанализированы: Федеральный Государственный Образовательный Стандарт высшего образования Российской Федерации, учебные пособия по информационной безопасности и защите информации, соответствующие научные публикации, рабочие программы по дисциплинам информационного цикла.

Преподавание теории и практики, оценивание результатов обучения проводилось на основе рабочей программы, соответствующей Федеральному Государственному Стандарту Российской Федерации Высшего Профессионального Образования, утвержденной в НОУ ВПО «Московская Академия Экономики и Права (рис. 3.3).

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НОУ ВПО «МОСКОВСКАЯ АКАДЕМИЯ ЭКОНОМИКИ И ПРАВА»

Институт экономики

Кафедра математики и информатики

УТВЕРЖДАЮ
Проректор по учебной работе
д.э.н., профессор
Малинина А.В.
12 февраля 2014 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Направление подготовки
080100.62 «Экономика»

Профиль подготовки
«Финансы и кредит»

Форма обучения
Очная, очно-заочная, заочная

Москва
2014

4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины «Защита компьютерной информации»составляет **3** зачетные единицы, **108** часов.

(очная форма обучения)

№ темы	Раздел дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
			Лекции	Практикум, Семинары	Самост. работа	
1	Теоретические основы методов и средств защиты компьютерной информации	3	1	1	4	опрос
2	Основы теории секретных систем	3		1	4	опрос
3	Классификация современных криптографических систем	3		1	4	опрос
4	Методы программной генерации псевдослучайных чисел	3	1	2	4	опрос
5	Блочные шифры	3		1	4	опрос
6	Режимы использования блочных шифров	3	1	2	4	опрос
7	Системы шифрования с открытым ключом	3		2	4	опрос
8	Вычислительные аспекты работы с простыми числами	3	1	2	4	Выполнение практических заданий
9	Электронная цифровая подпись. Алгоритмы Кеширования	3		2	4	Выполнение практических заданий
10	Криптографические протоколы	3	1	2	4	опрос
11	Стандарты шифрования	3		2	4	опрос
12	Системы защиты от копирования	3	1	2	4	Выполнение практических заданий
13	Методы защиты программного обеспечения от анализа и взлома	3		2	4	Выполнение практических заданий
14	Компьютерные вирусы и вредоносные программы	3	1	2	4	опрос
15	Компьютерная антивирусология	3		2	4	опрос
16	Сетевые атаки на информацию	3	1		4	опрос
17	Комплекс средств защиты от сетевых атак	3		2	8	Выполнение практических заданий
	Темы 1-17					Тестирование
	Итого: 108 часов		**8**	**28**	**72**	**Зачёт**

Рис. 3.3. Структура и содержание дисциплины «ЗКИ» 2014 г.

Теоретический материал преподавался на основе учебников по информационной безопасности Романцева Ю. В., Тимофеева П. А.[165], Мельникова В. П.[166], Шаньгина В. Ф.[167], Ярочкина В.И. [168] Практические работы проводились на основе методических указаний по защите компьютерной информации для математических и технических специальностей.

По окончании изучения дисциплины «Защита компьютерной информации» проведено анкетирование студентов экономического и юридического профилей подготовки Тираспольского филиала АНО ВО «Московская Академия экономики и права».

Анализ 57 анкет (Приложение 7) студентов показал, что 86% респондентов уверены в необходимости обучения основам информационной безопасности для своей будущей профессиональной деятельности, 10,5% не уверены в этом, 3,5% ответили отрицательно. В анкетах респонденты указывали процент посещенных занятий, свое

[165] РОМАНЦЕВ, Ю. В., ТИМОФЕЕВ, П. А., ШАНЬГИН, В. Ф. *Защита информации в компьютерных сетях*. Москва: Радио и связь. 2001. 375 с. ISBN 5-256-01518-4.

[166] МЕЛЬНИКОВ, В. П., КЛЕЙМЕНОВ, С. А., ПЕТРАКОВ, А. М. *Информационная безопасность и защита информации*. 3-е изд. Москва: Изд. центр «Академия», 2008. 336 с. ISBN 978-5-7695-4884-0.

[167] ШАНЬГИН, В.Ф. *Информационная безопасность компьютерных систем и сетей* Москва: ИД «ФОРУМ»: ИНФРА-М, 2012. 415 с. ISBN 978-5-8199-0331-5.

[168] ЯРОЧКИН, В.И. *Информационная безопасность*. 2-е изд. Москва: Академический проект; Гаудеамус. 2004. 544 с. ISBN 5-8291-0408-3.

отношение к предмету. Среди предложений чаще всего писали о расширении практической составляющей в области защиты информации (17,5%), об увеличении часов на изучение предмета (14,1%), об углублении знаний законодательных средств защиты информации (1,8%).

Анкетирование показало, что существующих дидактических средств недостаточно для формирования компетенций в области информационной безопасности у будущих экономистов.

Проведенный поисковый эксперимент позволил сделать следующие выводы:

1) будущие экономисты в большинстве своем осознают важность овладения теоретическими и практическими навыками в области защиты информации для своей профессиональной деятельности и личной жизни, а также хотели бы повысить свою подготовку;

2) программа обучения основам защиты компьютерной информации будущих экономистов должна отличаться от программы подготовки студентов, обучающихся по техническим специальностям;

3) при обучении будущих экономистов особое внимание необходимо уделить организационным и правовым средствам защиты;

4) практические занятия должны быть ориентированы на овладение необходимыми для будущей профессиональной деятельности навыками защиты компьютерной информации.

3.2.3 Констатирующий эксперимент

Констатирующий этап педагогического эксперимента реализовывался в 2015-2017 гг. с целью изучения современных подходов к обучению основам информационной безопасности будущих экономистов, определения методических ориентиров обучения информационной безопасности, формирования дидактической системы.

С учетом выводов, сделанных на предыдущем этапе эксперимента, корректировалась теоретическая и практическая часть курса «Защита компьютерной информации», изменена тематика теоретических занятий, разработаны практические занятия, формировался комплекс оценивающих средств. Разработана новая рабочая программа, учитывающая методические подходы к обучению будущих специалистов финансово-экономической сферы, основам информационной безопасности (Приложение 8). Обновленный дидактический комплекс сформирован средствами информационно-коммуникационных инструментов:

а) теоретическая часть:

– MS PowerPoint (программа подготовки презентаций) для создания

мультимедийных демонстраций по теоретическим материалам (2015 г.). Подготовленные мультимедийные демонстрации по ключевым темам курса необходимы для повышения наглядности на лекционных занятиях и для самостоятельной проработки теоретического материала;

– SunRav (программа создания электронных учебников) – создан электронный краткий курс лекций (2015 г.), необходимый для дополнительной самостоятельной проработки, в том числе и студентам заочной формы обучения, для работы в дистанционном режиме;

б) практическая часть:

– Joomag (цифровая платформа) – методические указания к практическим и лабораторным занятиям (2016 г.), публикации о проведенных деловых играх (2017 г.). Деловые игры являются одной из форм проектной деятельности. Методические указания в формате он-лайн журнала помогают организовать аудиторную работу в асинхронном режиме, отстающим студентам освоить практическую часть курса в ходе дополнительной проработки, студентам заочной формы обучения в дистанционном режиме;

в) оценивание:

– TestMoz (он-лайн конструктор тестов) для организации итогового (2015 г.) и текущего он-лайн тестирования (2016 г.), необходимого для получения обратной связи;

В констатирующем эксперименте принимали участие 74 человека: студенты второго курса экономического и юридического профилей подготовки Тираспольского филиала НОУ ВО «Московская Академия Экономики и Права» (ТФ НОУ ВО МАЭП) и студенты третьего курса ГОУ «Тираспольский Техникум Информатики и Права» (ТТИП), обучающиеся по направлению «Информационные системы в экономике». В ТФ НОУ ВО МАЭП читалась отдельная дисциплина «Защита компьютерной информации», в ТТИП в рамках дисциплины информационного цикла читался модуль «Защита компьютерной информации» (табл. 3.3).

Таблица 3.3. Результаты итогового тестирования по дисциплине «Защита компьютерной информации», 2015-2017 гг.

Учебный год	Учебное заведение	Направление подготовки	Группа	Кол-во, чел.	Средний балл по группе (100 балльная шкала)
2015-2016	МАЭП	Экономика	ЭД-14	13	31,9
2016-2017	МАЭП	Юриспруденция (заочное)	ЮЗ-12	20	24,6
2016-2017	ТТИП	Информационные системы в экономике	312	22	33,7
2016-2017	МАЭП	Юриспруденция	ЮД-15	19	24,8
Всего				74	

Всем студентам предоставлялся одинаковый теоретический материал, указания к выполнению практических работ, проводились деловые игры. Для оценки полученных

знаний по защите компьютерной информации проводилось итоговое тестирование, созданное на базе вопросов из имеющегося фонда оценочных средств.

Средний балл по исследуемым совокупностям рассчитан по формуле средней арифметической взвешенной (3.1), так как данные сгруппированы, и в каждой группе прошли итоговое тестирование разное количество студентов:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i * f_i}{\sum_{i=1}^{n} f_i} \qquad (3.1)$$

Подставив значения таблицы в формулу 3.1, получен средний балл:

$$\bar{x} = \frac{31{,}9 * 13 + 24{,}6 * 20 + 33{,}7 * 22 + 24{,}8 * 19}{31{,}9 + 24{,}6 + 33{,}7 + 24{,}8} = 28{,}6$$

Результаты итогового тестирования по дисциплине «Защита компьютерной информации» в 2015-2016 и 2016-2017 гг. среди студентов гуманитарного профиля подготовки показал, что обучающиеся в среднем ответили верно только на 28,6% вопросов, что является неудовлетворительным результатом. Это можно объяснить тем, что в наборе тестовых заданий особый акцент сделан на криптографические и технические средства защиты информации. В то время как на предыдущем этапе эксперимента были определены в качестве особых ориентиров обучения будущих экономистов основам информационной безопасности организационные и правовые средства защиты информации.

Проведенный констатирующий эксперимент позволил сделать следующие выводы:

1) дидактическая система обучения информационной безопасности будущих экономистов требует доработки, для получения более высоких результатов освоения;

2) в имеющемся наборе вопросов итогового тестирования в большей степени представлены темы, связанные с технической и криптографической защитой информации, и не выделены другие аспекты информационной безопасности;

3) необходимо создать комплексный тест, позволяющий провести всестороннюю оценку знаний будущих специалистов финансово-экономической сферы по защите компьютерной информации для обеспечения ее безопасности;

4) необходимо изменить рабочую программу по дисциплине «Защита компьютерной информации».

3.2.4 Уточняющий эксперимент

Уточняющий этап педагогического эксперимента реализовывался в 2017-2019 гг. с целью проверки и оптимизации построенной педагогической модели обучения информационной безопасности будущих экономистов с точки зрения кибернетического подхода с перспектив внедрения интернет технологий в процесс преподавание – учение – оценивание.

В рамках уточняющего эксперимента, в 2017-2019 уч. гг., реализовывались стратегические направления обучения будущих экономистов информационной безопасности, вносились коррективы в содержание учебно-методического комплекса, применялась проектная технология, отслеживались результаты, проверялась их эффективность в учебном процессе. Для самостоятельной проработки сложных моментов, вызывающих наибольшие затруднения у студентов, подготовлены видеоматериалы по ключевым темам курса. Для организации самостоятельной внеаудиторной деятельности применена образовательная технология – веб-квест.

В 2017-2018 гг. оптимизированы имеющиеся материалы и внедрены новые элементы в дидактическую систему обучения информационной безопасности будущих экономистов:

a) теоретическая часть:

– анимированные видеоролики по теоретической части курса в технике скрайбинг (2018 г.);

b) практическая часть:

– обновленные рекомендации к практическим занятиями (2018 г., 2019 г.);

c) оценивание:

– текущее тестирование в он-лайн конструкторе тестов TestMoz по теме «Электронно-цифровая подпись» (2018 г.);

– обновленное итоговое тестирование с выделенными уровнями сложности и разделением по темам изучаемого курса (2018 г.);

d) проектная деятельность:

– веб-квест по информационной безопасности, созданный на платформе GoogleSites и Google Forms (2017).

В каждом семестре были выделены две группы испытуемых с оказанием одинакового обучающего воздействия. Как таковой педагогической модели обучения информационной безопасности будущих экономистов еще не было. Материал одинаково преподавался в экспериментальной и контрольной группах. На этапе уточняющего эксперимента только начали искать методы, которые повысят эффективность преподавания в экспериментальной группе.

В 2017-2018 гг. были подготовлены видеоматериалы по наиболее сложным моментам преподаваемой дисциплины. Их студенты могли использовать при подготовке домашних заданий, актуализации знаний, при самостоятельном изучении.

На этапе уточняющего эксперимента применялись проектные методы обучения: веб-квесты и деловые игры. Оценивание студентов проводилось с использованием

балльно-рейтинговой системы, важную часть которой составляет промежуточная аттестация, осуществляемая при помощи итогового тестирования.

Статистический анализ результатов итогового тестирования в рамках уточняющего эксперимента 2017-2018, 2018-2019 гг. состоит из: 1) определения средних, стандартного отклонения и медианы в каждой группе (табл. 3.4); 2) проверки гипотезы о равенстве средних с помощью критерия Манна-Уитни (табл. 3.5).

Исходные данные уточняющего эксперимента (Приложение 10) и расчет описательных характеристик проведен средствами SPSS (Приложение 11).

Таблица 3.4. Основные статистические показатели для выборок, участвовавших в уточняющем эксперименте

Год, семестр	Группа	Выборка	Количество студентов	Среднее	Медиана	Стандартное отклонение	Коэффициент вариации	Коэффициент асимметрии
2017-2018 осенний семестр	ТФ МАЭП Экономисты	ЭГ-1	18	39,44	38,0	16,978	43,0	0,540
	ТФ МАЭП Менеджеры	КГ-1	7	30	29,0	10,924	34,3	0,672
2017-2018 весенний семестр	ТТИП Прикладная информатика в экономике	ЭГ-2	13	44,15	45,0	13,771	31,2	-0,687
	ТТИП Прикладная информатика в экономике	КГ-2	18	41,89	43,0	14,483	34,6	-0,138
2018-2019 осенний семестр	ТФ МАЭП Экономисты	ЭГ-3	9	41,44	39,0	14,993	36,2	0,375
	ТФ МАЭП Менеджеры	КГ-3	22	43.14	42,0	13,464	31,2	0,436
Итого			87					

Средняя величина представляет обобщенную характеристику индивидуальных значений количественного признака в конкретных условиях места и времени [169, с. 42], медиана (Ме) – серединное значение признака в ранжированном ряду [там же, с. 49]. Стандартное отклонение, определяемое как корень из дисперсии, является мерой разброса значений в представленном множестве от средней величины множества. Коэффициент вариации – это относительный показатель разброса значений множества от средней величины этого множества. Чем коэффициент вариации выше, тем совокупность неоднороднее. Коэффициент асимметрии характеризует степень асимметричности

[169] ИВЧЕНКО, Ю. С. *Статистика*. Москва: РИОР:ИНФРА-М, 2011. 375 с. ISBN 978-5-369-00636-8

распределения относительно средней величины.

Анализ статистических данных, представленных в таблице 3.4, свидетельствует о различии полученных результатов экспериментальной и контрольной групп. Среднее значение результата тестирования и медиана выше в экспериментальных группах по сравнению с контрольными группами. Коэффициент вариации практически во всех сериях выше 33%, что свидетельствует о неоднородности выборок. Коэффициент асимметрии подтверждает отклонение медианного значения от среднего балла, полученного в ходе итогового тестирования.

Оценим значимость различия средних в экспериментальных и контрольных группах при помощи непараметрического критерия Манна-Уитни. Выбор непараметрического критерия Манна-Уитни обусловлен тем, что количество наблюдений в каждой выборке меньше 30, поэтому нет возможности оценить распределение на нормальность и применить t-критерий Стьюдента.

Сформулируем нулевую и альтернативную гипотезы.

H_0: результаты обучения в ЭГ и КГ статистически не отличаются друг от друга.

H_1: результаты обучения в ЭГ и КГ статистически различны.

Анализ результатов исследования с помощью критерия Манна-Уитни проведен в SPSS (Приложение 12) и представлен в таблице 3.5.

Таблица 3.5. Критерий Манна-Уитни, для выборок, участвовавших в уточняющем эксперименте

Год, семестр	Группа	Выборка	Количество студентов	Критерий Манна Уитни	Табличное значение	Значимость	Принимается гипотеза α=0,05
2017-2018 осенний семестр	ТФ МАЭП Экономисты	ЭГ-1	18	41	35	0,198	H_o
	ТФ МАЭП Менеджеры	КГ-1	7				
2017-2018 весенний семестр	ТТИП Прикладная информатика в экономике	ЭГ-2	13	109	75	0,767	H_o
	ТТИП Прикладная информатика в экономике	КГ-2	18				
2018-2019 осенний семестр	ТФ МАЭП Экономисты	ЭГ-3	9	105,5	60	0,781	H_o
	ТФ МАЭП Менеджеры	КГ-3	22				

Три серии уточняющего эксперимента, отраженные в таблице 3.5, показали, что различия в средних оценках экспериментальных и контрольных групп статистически

незначимы. Рассчитанные значения критерия Манна-Уитни больше табличного значения во всех трех сериях испытаний на уровне значимости α=0,05, что свидетельствует о необходимости принять гипотезу H_o об отсутствии существенных различий в результатах обучения в экспериментальных и контрольных группах. О необходимости принять нулевую гипотезу свидетельствует и асимптотическая значимость, уровень которой в каждой серии выше 0,05.

Можно сделать вывод, что на этапе уточняющего эксперимента применение предложенных методов и средств обучения позволили получить статистически достоверно одинаковый результат учебной деятельности в экспериментальной и контрольной группах.

При чтении лекций в экспериментальной и контрольной группах применялись одинаковые информационно-коммуникационные средства, одинаковые приложения, поэтому не было ожидаемой эффективности.

Проведенный уточняющий эксперимент позволил сделать следующие выводы:

1) необходимо построить педагогическую модель обучения информационной безопасности будущих экономистов для повышения эффективности преподавания и проверить ее в экспериментальной группе на этапе формирующего эксперимента;

2) необходимо оценить влияние применения проектных методов обучения на результаты обучения информационной безопасности будущих экономистов.

3.3 Проверка эффективности педагогической модели на формирующем этапе

3.3.1 Статистический анализ значимости результатов

Формирующий этап педагогического эксперимента реализовывался в 2019-2020 учебном году и осеннем семестре 2020-2021 учебного года с целью подтверждения гипотезы о значимости спроектированной дидактической системы по обучению технологиям защиты информации для обеспечения ее безопасности будущих специалистов финансово-экономической сферы, повышения результативности учебной деятельности.

В формирующий эксперимент, состоящий из трех серий испытаний, были вовлечены в общей сложности 55 студентов. Для проверки результативности формирующего эксперимента проводилось итоговое тестирование экспериментальной и контрольной групп.

В экспериментальные группы (ЭГ) входили студенты Тираспольского филиала АНО ВО «Российский Новый Университет» (22 чел.):

– 2019-2020 уч. г. осенний семестр группы ТИ19ПИ направление «Прикладная

информатика в экономике» 5 чел.;

– 2019-2020 уч. г. весенний семестр группы ТИ19ЭФБ направление «Экономика» 7 чел.;

– 2020-2021 уч. г. осенний семестр группы ТИ20ЭФБ направление «Экономика» 10 чел.

В контрольные группы (КГ) входили студенты Бендерского Политехнического Филиала ПГУ им. Т.Г. Шевченко (33 чел.):

– 2019-2020 уч. г. осенний семестр группы БП17ВР62ЭПиОС1 направление «Экономика» 6 чел.;

– 2019-2020 уч. г. весенний семестр 26 группы направление «Информационные системы в экономике» 17 чел.;

– 2020-2021 уч. г. осенний семестр группы БП18ДР62ЭК1 направление «Экономика» 10 чел.

Отметим, что экспериментальные и контрольные группы находились в равных условиях в части освоения практических и теоретических навыков. В экспериментальной группе были созданы специальные условия, положительно влияющие на результативность учебной деятельности: проектный метод, видеолекции, текущее тестирование.

Применение проектного метода в системе обучения информационной безопасности будущих экономистов необходимо для расширения возможностей освоения теоретического материала, овладения практическими навыками, и, следовательно, повышение результативности эксперимента. В экспериментальных группах была организована научно-исследовательская деятельность студентов (участие в студенческих конференциях, подготовка мультимедийных демонстраций), реализован проект «Цифровая грамотность людей старшего возраста» (студенты составляли вопросы, формировали анкету GoogleForms, проводили анкетирование, снимали видеоматериалы учебного характера).

Текущее тестирование в экспериментальной группе проводилось для получения обратной связи о степени освоения ключевых тем изучаемой дисциплины. Каждый текущий тест содержал 3-5 вопросов, анализ ответов позволял выявить возникшие сложности в освоении материла, как всеми обучающимися, так и отдельно взятыми студентами. В учебном процессе использовались видеоматериалы, освещающие сложные элементы курса.

По итогам прохождения курса «Информационная безопасность» студенты контрольных и экспериментальных групп выполнили итоговый тест, в котором представлены 36 вопросов по 6 основным разделам изучаемой дисциплины:

Раздел I. Основные понятия и угрозы информационной безопасности.

Раздел II. Законодательные средства информационной безопасности.

Раздел III. Средства защиты компьютерной информации.

Раздел IV. Идентификация и аутентификация. Пароли.

Раздел V. Основы криптографии.

Раздел VI. Электронно-цифровая подпись и алгоритмы хеширования.

В каждом разделе представлены вопросы четырех уровней сложности (Приложение 6). Анализ результатов итогового тестирования в разрезе уровней сложности представлен в таблице 3.6.

Таблица 3.6. Средний балл итогового тестирования в разрезе уровней сложности

Год, семестр	Выборка	Уровень сложности			
		I	II	III	IV
2019-2020 осенний семестр	ЭГ	78,0	56,5	68,9	83,5
	КГ	71,0	53,0	48,2	73,9
2019-2020 весенний семестр	ЭГ	84,3	65,8	77,1	81,6
	КГ	64,6	42,8	41,6	63,3
2020-2021 осенний семестр	ЭГ	74.4	52.7	65,3	77,4
	КГ	72,6	54,4	58,2	72,9

Из таблицы 3.6 и графиков, представленных на рис.3.4-3.6, видно, что результаты итогового тестирования по каждому уровню сложности в экспериментальных группах выше, чем в контрольных во всех сериях экспериментального исследования.

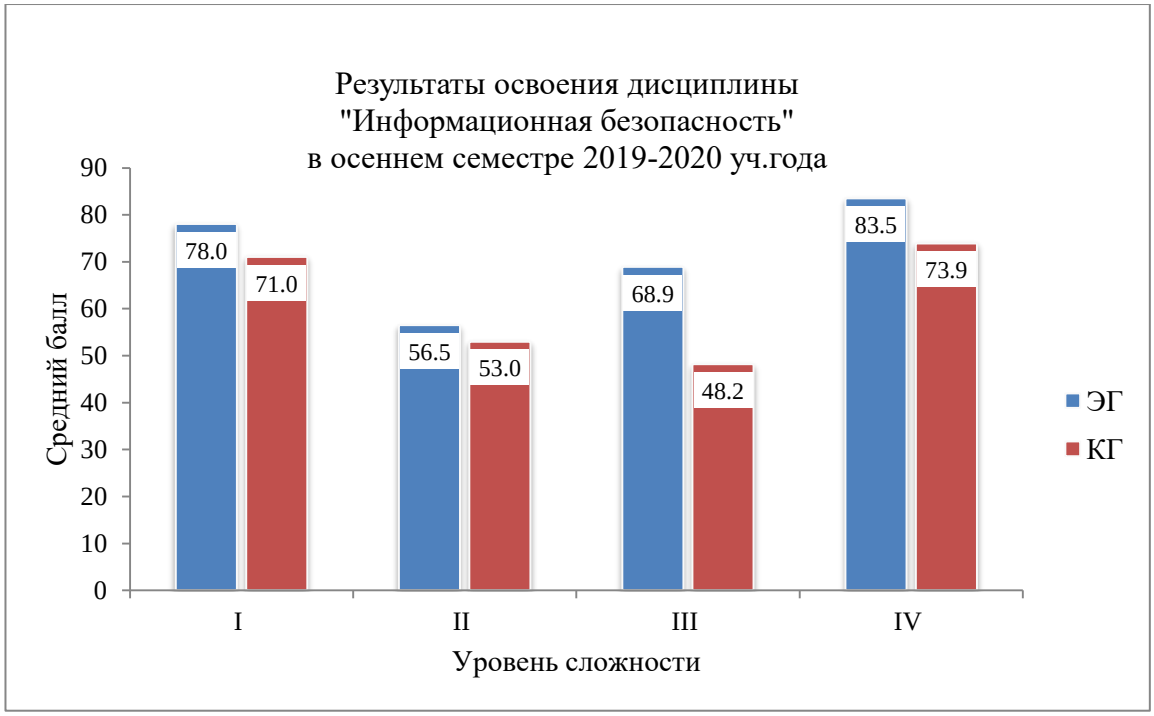


Рис. 3.4. Результаты освоения дисциплины "Информационная безопасность" в осеннем семестре 2019-2020 уч. года

В осеннем семестре 2019-2020 уч. г. с вопросами первого уровня сложности

справились 78% студентов экспериментальной группы и 71% – контрольной. Со вторым уровнем сложности справились 56,5% студентов экспериментальной группы и 53% – контрольной. С третьим уровнем сложности справились 68,9% студентов экспериментальной группы и 48,2% – контрольной. С четвертым уровнем сложности справились 83,5% студентов экспериментальной группы и 73,9% – контрольной.

Низкий уровень оценок по второму уровню объясняется тем, что вопросы в основном представлены в виде множественного выбора. В таком типе вопросов если хотя бы один из правильных вариантов не отмечен, либо, наоборот, отмечен лишний вариант, то балл за ответ значительно снижается. Высокий балл по четвертому уровню объясняется тем, что там чаще всего представлены вопросы открытого типа, оцениваемый выше остальных. Вопросы сформулированы с однозначной трактовкой, указано количество букв в слове, в системе TestMoz записаны все варианты написания правильного ответа. Поэтому студенты допустили небольшое количество ошибок при ответах на вопросы четвертого уровня сложности.

Аналогичные выводы делаем по данным, полученным в ходе итогового тестирования для весеннего семестра 2019-2020 уч. г. и осеннего семестра 2020-2021 уч. г.

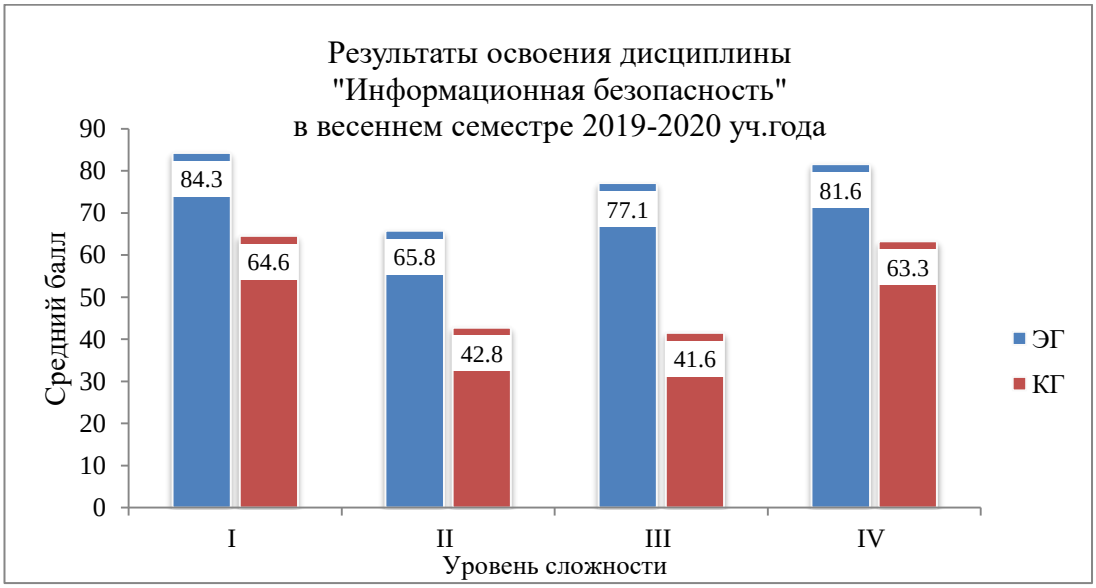


Рис. 3.5. Результаты освоения дисциплины "Информационная безопасность" в весеннем семестре 2019-2020 уч. года

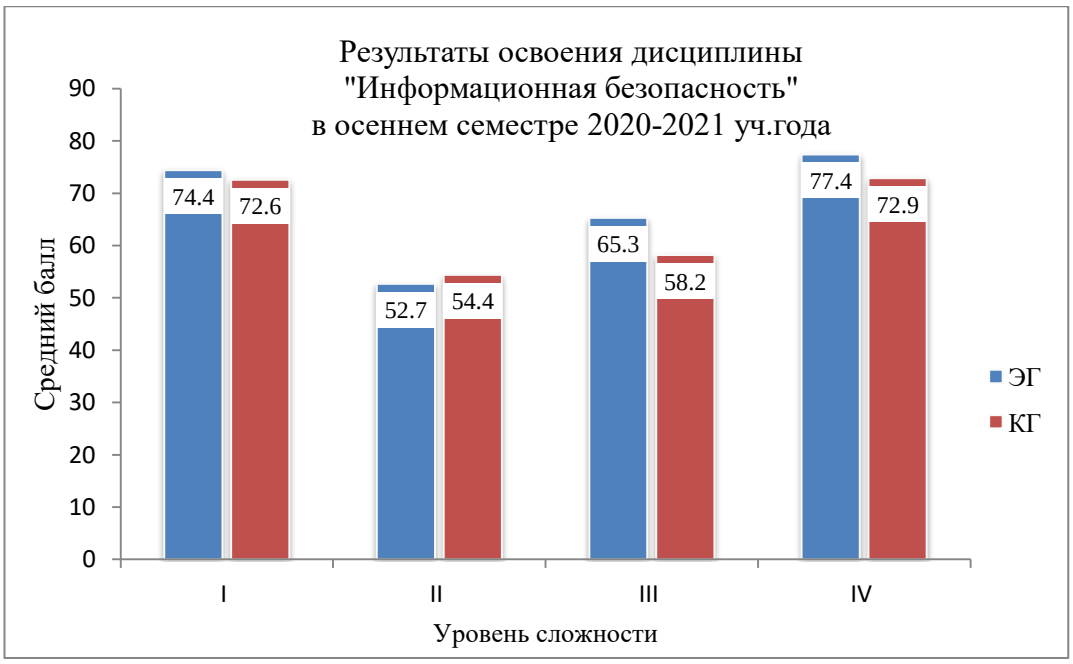


Рис. 3.6. Результаты освоения дисциплины "Информационная безопасность" в осеннем семестре 2020-2021 уч. года

Оценивание результатов итогового тестирования произведено средствами он-лайн конструктора TestMoz.com, данные экспортированы в MS Excel и обработаны в SPSS (Приложение 13). Основные статистические показатели результатов итогового тестирования в трех сериях формирующего эксперимента представлены в Приложении 14 и сведены в таблицу 3.7.

Таблица 3.7. Основные статистические показатели формирующего эксперимента

Год, семестр	Выборка	Количество студентов (n)	Среднее (m)	Медиана	Стандартное отклонение (σ)	Коэффициент вариации ($R_σ$), %	Асимметрия
2019-2020 осенний семестр	ЭГ	5	71,20	72,00	5,263	7,4	-0.959
	КГ	6	60,50	60,50	4,680	7,7	-0,176
2019-2020 весенний семестр	ЭГ	7	77,00	79,00	7,439	9,7	-1,007
	КГ	17	53,71	57,00	11,746	21.9	-0,272
2020-2021 осенний семестр	ЭГ	10	75,00	75,00	11,353	15,1	0,017
	КГ	10	59,90	63,00	13,511	22,6	-0,368
Итого		55					

В таблице 3.7 отображены такие статистические показатели как: среднее значение, медиана, стандартное отклонение и коэффициент вариации, асимметрия. Коэффициент вариации – отношение среднего значения к стандартному отклонению – свидетельствует об однородности всех групп по показателю оценка, т.к. его значение для каждой группы меньше 33%. Отрицательные значения асимметрии для экспериментальной и контрольной групп (кроме ЭГ 2020-2021 уч. г.) указывает на сдвиг распределения относительно

среднего значения в сторону больших значений. Для ТФ РОСНОУ в 2019-2020 уч.г. – сдвиг в сторону меньших значений, и распределение не является нормальным, т.к. асимметрия выходит за пределы интервала [-1;1].

Различия в средних значениях оценок в ЭГ и КГ в каждой серии формирующего эксперимента (рис. 3.7) позволяет предположить эффективность спроектированной дидактической системы в обучении технологиям защиты информации для обеспечения ее безопасности будущих специалистов финансово-экономической сферы.

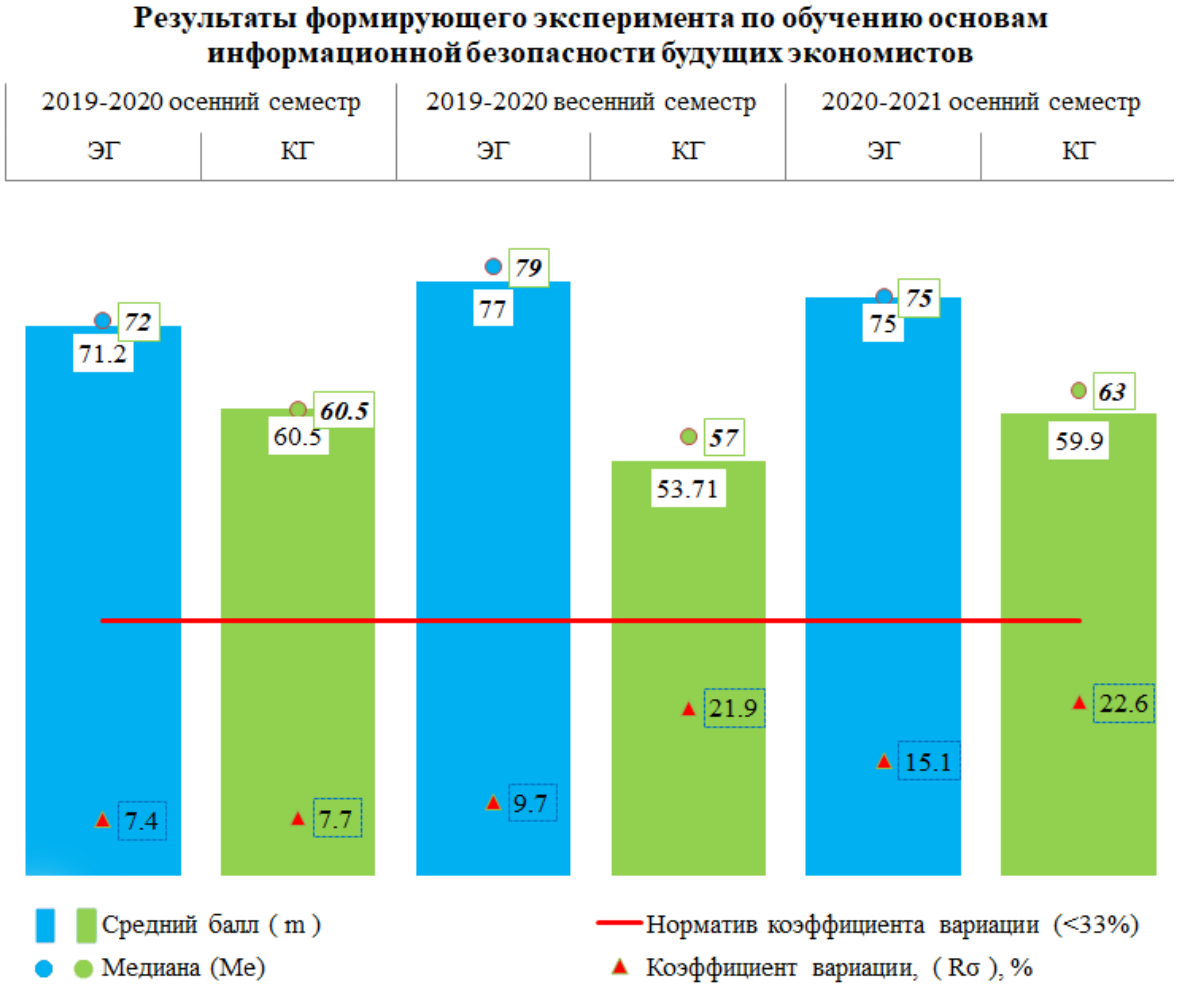


Рис. 3.7. Статистические показатели формирующего эксперимента по ЭГ и КГ

Необходимо проверить значимость полученных различий с помощью статистических критериев. Характер имеющихся выборок (2 независимые выборки в каждой серии, меньше 30 наблюдений в каждой группе) предполагает применение непараметрических критериев.

Оценим статистическую значимость различий полученных результатов итогового тестирования в ЭГ и КГ с помощью непараметрических критериев *U*-Манна-Уитни и ϕ^*– углового преобразования Фишера.

3.3.2 Оценка значимости результатов по U-критерию Манна-Уитни

Для применения непараметрического *U*-критерия Манна-Уитни выполняется условие, что в каждой выборке не менее 3 наблюдений, и не требуется нормальное распределение наблюдений [170, 171, 172].

U-критерий Манна-Уитни в отличие от большинства других критериев предполагает, что статистические различия существенны, если эмпирическое значение ($U_{эмп}$) меньше критического ($U_{крит}$). Т.е. нулевая гипотеза H_0 о статистической незначимости различий между средними значениями в двух выборках принимается на уровне значимости *p*, если $U_{эмп}>U_{крит}$. И, наоборот, альтернативная гипотеза H_1 о статистической значимости различий между средними значениями в двух выборках принимается на уровне значимости *p,* если $U_{эмп}<U_{крит}$.

Эмпирические значения *U*-критерия Манна-Уитни рассчитаны по формуле 3.2:

$$U_i = n_1 * n_2 + \frac{n_i(n_i+1)}{2} - R_i \qquad (3.2)$$

где R_i –сумма рангов для i-ой выборки; n_1 и n_2– количество наблюдений в 1-ой и 2-ой группах.

В таблице 3.7 приведены значения средних баллов в ЭГ и КГ: m_1=71,2 и m_2=60,5. Оценим статистическую значимость различия средних в исследуемых группах при помощи непараметрического *U*-критерия Манна-Уитни для осеннего семестра 2019-2020 уч.г. в рамках формирующего эксперимента.

Сформулируем нулевую и альтернативную гипотезы.

H_0: результаты обучения в ЭГ и КГ статистически не отличаются друг от друга.

H_1: результаты обучения в ЭГ и КГ статистически различны.

Результаты, полученные студентами обеих групп в ходе итогового тестирования, объединены в один вариационный ряд и упорядочены по возрастанию (табл. 3.8).

Таблица 3.8. Ранжированные результаты итогового тестирования в КГ и ЭГ в осеннем семестре 2019-2020 уч.г.

ЭГ группа (n_1=5)	Балл	Ранг	КГ группа (n_2=6)	Балл	Ранг
			КГ	54	1
			КГ	57	2
			КГ	59	3
			КГ	62	4
ЭГ	63	5			

[170] ГУБЛЕР, Е. В. *Вычислительные методы анализа и распознавания патологических последствий*. Ленинград: Медицина, 1978. 295 с.
[171] УРБАХ, В. Ю. *Статистический анализ в биологических и медицинских исследованиях*. Москва: Медицина, 1975. 297 с.
[172] СИДОРЕНКО, Е.В. *Методы математической обработки в психологии*. Санкт-Петербург: ООО «Речь», 2000. 350с. ISBN 5-9268-0010-2.

			КГ	65	6
			КГ	66	7
ЭГ	70	8			
ЭГ	72	9			
ЭГ	74	10			
ЭГ	77	11			
Сумма рангов		43			23

Вычислена сумма рангов отдельно для ЭГ (R_1=43) и для КГ (R_2=23). Общая сумма рангов: 43+23=66. Расчетная сумма (4): $\sum R_i = 66$. Равенство реальной и расчетных сумм соблюдено.

Значение критерия Манна-Уитни для ЭГ (U_1) и КГ (U_2) рассчитывают по формуле (3.2):

$$U_1 = n_1 * n_2 + \frac{n_1(n_1+1)}{2} - R_1 = 5 * 6 + \frac{5(5+1)}{2} - 43 = 2$$

$$U_2 = n_1 * n_2 + \frac{n_2(n_2+1)}{2} - R_2 = 5 * 6 + \frac{6(6+1)}{2} - 23 = 28$$

Из двух эмпирических критериев выбираем наименьший, т.е. $U_{эмп}$.=2 и сравниваем с табличным значением.

По специальным таблицам [173, с. 316], определим критические значения критерия Манна-Уитни для уровней статистической значимости p=0,01 и p=0,05 для n_1=5 и n_2=6: $U_{0,01}\,(5;6) = 2$ и $U_{0,05}\,(5;6) = 5$.

Т.к. рассчитанное значение U-критерия равно критическому при p=0,01, а именно $U_{эмп}$= 2 ≤ 2= $U_{крит}$, то H_0 отвергается с вероятностью 99% и принимается альтернативная гипотеза H_1, свидетельствующая о статистической достоверности различий между средним баллом в ЭГ и КГ (рис. 3.8).

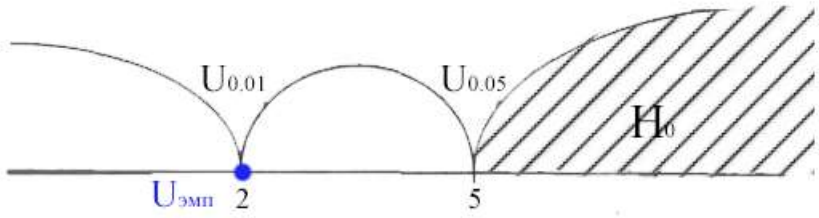


Рис. 3.8. Область принятия гипотезы *U*-критерия

Критические значения критерия Манна-Уитни U_p (n_1, n_2) определены по таблицам [174, с. 316; 175, с. 90] для n_1 и n_2 и уровней значимости p=0,01 и p=0,05 и внесены в таблицу 3.9.

---

[173] Там же

[174] Там же

[175] ЛАКИН, Г. Ф. *Биометрия*. Москва: Высшая Школа, 1990, 352 с. ISBN 5-06-000471-6.

Результаты произведенного в программе SPSS расчета *U*-критерия Манна-Уитни для трех серий формирующего эксперимента представлены в Приложении 14 и сведены в таблицу 3.9.

Таблица 3.9. Критерий Манна-Уитни для выборок формирующего эксперимента

Год, семестр	Выборка	Количество студентов	$U_{эмп}$	$U_{0.01}$	$U_{0.05}$	Значимость *p*	Гипотеза
2019-2020 осенний семестр	ЭГ	n_1=5	**2**	**2**	5	0,017	H_1
	КГ	n_2=6					
2019-2020 весенний семестр	ЭГ	n_1=7	**4**	**23**	33	0,000	H_1
	КГ	n_2=17					
2020-2021 осенний семестр	ЭГ	n_1=10	**21**	19	**27**	0,029	H_1
	КГ	n_2=10					
Итого		55					

Анализируя данные таблицы 3.9, видим, что в каждой серии формирующего эксперимента подтверждается гипотеза H_1. Об этом свидетельствуют полученные в каждой серии $U_{эмп}<U_{крит}$.

По результатам итогового тестирования в осеннем семестре 2019-2020 уч. г. определено, что $U_{эмп}= 2 \leq 2= U_{0.01}$ (5;6), т. е. гипотеза H_0 отвергается, и принимается альтернативная гипотеза H_1 на уровне значимости p=0.017, свидетельствующая о существовании статистически значимых различий между средним баллом в ЭГ и КГ.

По результатам итогового тестирования в весеннем семестре 2019-2020 уч. г. определено, что $U_{эмп}= 4 \leq 23= U_{0.01}$(7;17), т.е. гипотеза H_0 отвергается и принимается альтернативная гипотеза H_1 на уровне значимости p=0.000, свидетельствующая о существовании статистически значимых различий между средним баллом в ЭГ и КГ.

По результатам итогового тестирования в осеннем семестре 2020-2021 уч. г. определено, что $U_{эмп}= 21 \leq 27= U_{0.05}$(10;10), т. е. гипотеза H_0 отвергается и принимается альтернативная гипотеза H_1 на уровне значимости p=0.029, свидетельствующая о существовании статистически значимых различий между средним баллом в ЭГ и КГ.

Можно сделать вывод, что уровень обученности (средний балл) в ЭГ статистически значимо выше, чем уровень обученности в КГ на уровне значимости $p=0,05$ в каждой серии формирующего эксперимента (рис. 3.9).

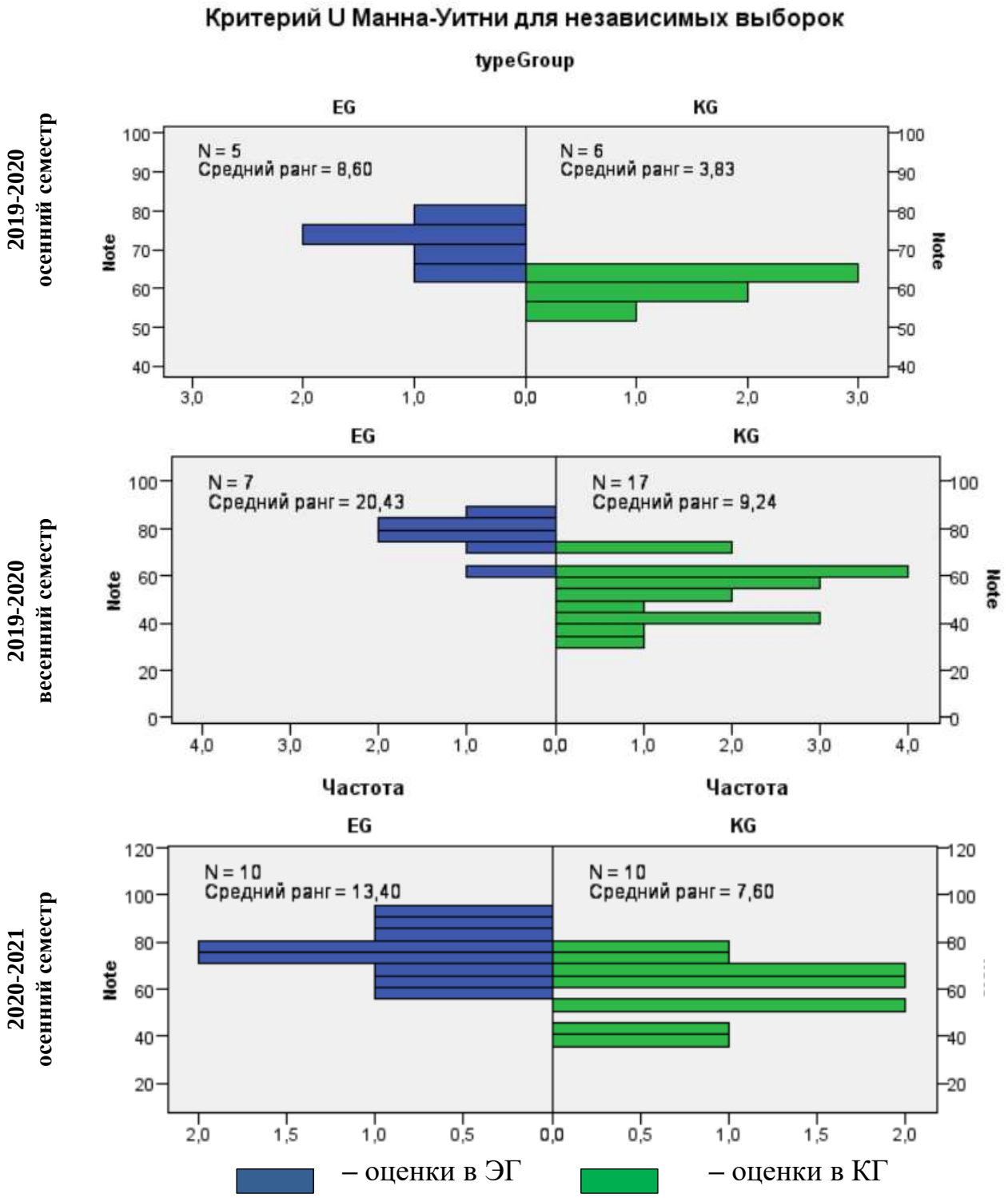


Рис. 3.9. Значения *U*-критерия в трех сериях формирующего эксперимента

3.3.3 Оценка значимости результатов по φ–критерию Фишера*

Исследование малых выборок с неопределенным распределением эффективно проводить с помощью непараметрических критериев. Методология обработки педагогической информации с помощью φ*–критерия углового преобразования Фишера

подробно рассмотрена в работе [176].

Оценка значимости полученных результатов итогового тестирования проверена с помощью непараметрического $\boldsymbol{\varphi}$*–критерия углового преобразования Фишера. Для его применения необходимо использовать только альтернативные значения признака, и в каждой выборке должно быть не менее 5 наблюдений. В ходе итогового тестирования студент может набрать максимум 100 баллов. За признак «есть эффект» примем верный ответ на 2/3 и более вопросов (66 баллов и более), а за признак «нет эффекта» – менее 2/3 вопросов (менее 66 баллов).

При составлении итогового теста вопросы подготовлены таким образом, что если студент набирает 66 баллов и более, то можно считать, что он владеет материалом на более качественном уровне. Таким образом, 66 баллов и более были выбраны в качестве критерия достижения эффекта.

Сформулируем гипотезы:

H_o: доля студентов набравших 66 баллов и более в ЭГ не больше, чем в КГ.

H_1: доля студентов набравших 66 баллов и более в ЭГ больше, чем в КГ.

Вычисление эмпирического значения $\varphi^*_{\text{эмп}}$ произведем по формуле (3.3) [177, стр. 162; 178, стр.166]:

$$\varphi^*_{\text{эмп}} = (\boldsymbol{\varphi_1} - \boldsymbol{\varphi_2}) * \sqrt{\frac{n_1 * n_2}{n_1 + n_2}} \quad (3.3)$$

где φ_1 – угол, соответствующий большей % доле; φ_2 – угол, соответствующий меньшей % доле; n_1 – количество наблюдений в выборке 1; n_2 – количество наблюдений в выборке 2.

Значение φ_i можно найти по справочным таблицам либо по формуле (3.4) [Сидоренко Е. В., с.159; Урбах В. Ю., с.154]:

$$\varphi_i(P_i) = 2 * \arcsin\sqrt{P_i} \quad (3.4)$$

где P_i – это процентная доля эффекта в каждой группе; i – номер выборки.

В математической статистике принято задавать уровень значимости (вероятность ошибки) p=0,05, p=0,01 и p=0,001, что соответствует достоверности результатов в 95%, 99% и 99,9% [179].

---

[176] БОГДАНОВА, В. А. Методология обработки педагогической информации с помощью критериев ф*-углового преобразования Фишера и Манна-Уитни. In: *Revista Univers Pedagogic*. 2021, Nr.3 (71), с. 56-63. doi.org/10.52387/1811-5470.2021.3.07. ISSN 1811-5470

[177] СИДОРЕНКО, Е.В. *Методы математической обработки в психологии*. Санкт-Петербург: ООО «Речь», 2000. 350с. ISBN 5-9268-0010-2.

[178] УРБАХ, В. Ю. *Статистический анализ в биологических и медицинских исследованиях*. Москва: Медицина, 1975. 297 с.

[179] ГУБЛЕР, Е. В. *Вычислительные методы анализа и распознавания патологических последствий*. Ленинград: Медицина, 1978. 295 с.

Критическое значение $\varphi^*_{\text{кр}}$ определены по справочным таблицам для уровня значимости p=0.01 и p=0.05. Табличное значение критерия запишем как формулу (3.5):

$$\varphi^*_{\text{кр}} = \begin{cases} 1{,}64 \text{ для } p = 0{,}05 \\ 2{,}31 \text{ для } p = 0{,}01 \end{cases} \quad (3.5)$$

Таким образом, критическое значение φ^*–критерия углового преобразования Фишера определены по справочным таблицам [Сидоренко Е.В., с. 162; Урбах В. Ю., с.159]: $\varphi^*_{0,01} = 2{,}31$ для уровня значимости p=0,01 и $\varphi^*_{0,05} = 1{,}64$ для p =0,05. Для принятия решения о статистической достоверности эмпирическое значение сравнивают с критическим заданного уровня значимости.

Если $\varphi^*_{\text{эмп}} < \varphi^*_{\text{крит}}$, то с вероятностью $1 - p$ принимается гипотеза H_0 о статистической незначимости различий в исследуемых группах, т.е. доли испытуемых достигших «эффекта» в обеих выборках статистически не различаются.

Если $\varphi^*_{\text{эмп}} > \varphi^*_{\text{крит}}$, то с вероятностью $1 - p$ отклоняется гипотеза H_0, и принимается гипотеза H_1 о том, что доля испытуемых, достигших «эффекта», в ЭГ статистически достоверно больше, чем в КГ.

В рамках формирующего этапа педагогического эксперимента, – по обучению информационной безопасности будущих специалистов финансово-экономического сектора, – в осеннем семестре 2019-2020 уч. г. проведено итоговое тестирование студентов экспериментальной группы (ЭГ) ТФ АНО ВО «Российский Новый Университет» (5 чел.) и контрольной группы (КГ) Бендерского Политехнического Филиала ПГУ им. Т.Г. Шевченко (6 чел.). Небольшое количество наблюдений не позволяет применить параметрические критерии, требующие нормального распределения.

Для применения φ^*-критерия углового преобразования Фишера выполняется условие, что в каждой выборке не менее 5 наблюдений.

Ограничением критерия является использование только альтернативных значений признака. За признак «есть эффект» примем верный ответ на 2/3 и более вопросов итогового тестирования (66 баллов и более), а за признак «нет эффекта» – менее 2/3 вопросов (менее 66 баллов из 100 возможных).

Вычислим процентные доли как соотношение одной части совокупности ко всей совокупности. Например, в ЭГ 4 студента из 5 (80%) набрали более 66 баллов по итоговому тестированию, а в КГ – только 1 студент из 6 (16,7%). Полученные баллы, процентные доли (P_i) и средние значения по группам (m_i) представлены в Таблице 3.10.

Таблица 3.10. Результаты итогового тестирования по дисциплине «Информационная безопасность» в осеннем семестре 2019-2020 уч. г.

Изучаемый признак	Группа			
	Экспериментальная группа (ЭГ)		Контрольная группа (КГ)	
	Балл	Доля, % (P_i)	Балл	Доля, % (P_i)
Есть эффект, *mark ≥ 66*	70, 72, 74, 77	80%	66	16.7 %
Нет эффекта, *mark ≤ 66*	63	20%	54, 57, 59, 62, 65	83,3%
Суммы	356 баллов	100%	363 балла	100%
Средние	m_1=71,2		m_2=60,5	

Сформулируем гипотезы:

H_o: доля студентов набравших 66 баллов и более в ЭГ не больше, чем в КГ.

H_1: доля студентов набравших 66 баллов и более в ЭГ больше, чем в КГ.

Построим четырехклеточную таблицу эмпирических частот по двум значениям признака «есть эффект» и «нет эффекта» (таблица 3.11).

Таблица 3.11. Таблица сопряженности результатов итогового тестирования осеннего семестра 2019-2020 уч. г.

Группа	Изучаемый признак						Итого, чел.
	Есть эффект, *mark ≥ 66*			Нет эффекта, *mark ≤ 66*			
	Количество человек	Доля, %		Количество человек	Доля, %		
ЭГ	4	**80%**	А	1	20 %	Б	n_1=5
КГ	1	**16,7%**	В	5	83,3%	Г	n_2=6
Итого	5			6			11

Выбираем данные, участвующие в сопоставлении: «есть эффект» в ЭГ (А) и «есть эффект» в КГ (В). Вычислим величины φ_i, соответствующие процентным долям «эффекта» в каждой из групп по формуле 3.4:

$$\varphi_1(80\%) = 2 * \arcsin\sqrt{0.8} = 2{,}214$$

$$\varphi_2(16{,}7\%) = 2 * \arcsin\sqrt{0{,}167} = 0{,}841.$$

Эти же значения можно найти в статистических таблицах $\boldsymbol{\varphi}$*–критерия углового преобразования Фишера.

Вычислим эмпирическое значение $\varphi^*_{\text{эмп}}$ по формуле 3.3:

$$\varphi^*_{\text{эмп}} = (2{,}214 - 0{,}841) * \sqrt{\frac{5 * 6}{5 + 6}} = 2{,}27$$

Полученному значению 2,27, согласно учебнику Сидоренко Е. В., соответствует уровень значимости *p=0,012*, т. е. вероятность ошибки составляет 1,2%. Т.к. эмпирическое значение больше критического (условие принятия гипотезы H_1):

$$\varphi^*_{\text{эмп}} = 2{,}27 \geq 1{,}64 = \varphi^*_{\text{крит}},$$

то гипотеза H_0 отвергается, и принимается гипотеза H_1 о том, что доля студентов набравших 66 баллов и более в ЭГ больше, чем в КГ с вероятностью 98,8 % (рис. 3.10).

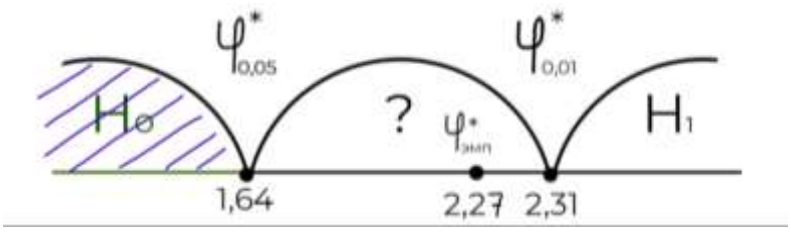


Рис. 3.10. Область принятия гипотезы *φ-критерия**

Аналогично рассчитан *φ**-критерия углового преобразования Фишера для подтверждения статистической значимости различия результатов итогового тестирования по дисциплине «Информационная безопасность», проведенного в ЭГ и КГ в весеннем семестре 2019-2020 уч. г. и осеннем семестре 2020-2021 уч. г.. Данные трех серий формирующего эксперимента сведены в таблицу 3.12.

Таблица 3.12. Расчет эмпирического φ*-критерия углового преобразования Фишера

№	Показатель	Обозначение	2019-2020 осенний семестр	2019-2020 весенний семестр	2020-2021 осенний семестр
1	Количество человек в ЭГ	n1	5	7	10
2	Количество человек в КГ	n2	6	17	10
3	Доля студентов, набравших 66 баллов и более	P_1	80%	85,7%	80%
4	Доля студентов, набравших менее 66 баллов	P_2	16,7%	11,8%	20%
5	угол, соответствующий большей % доле	$\varphi_1(P_1) = 2 * \arcsin\sqrt{P_1}$	2,214	2,456	2,214
6	угол, соответствующий меньшей % доле	$\varphi_2(P_2) = 2 * \arcsin\sqrt{P_2}$	0,839	0,701	1,369
7	**эмпирическое значение**	$\varphi *= (\varphi_1 - \varphi_2) * \sqrt{\frac{n_1 * n_2}{n_1 + n_2}}$	**2,27**	**3,91**	**1,89**

Сравнив рассчитанный (эмпирический) *φ**-критерий углового преобразования Фишера и табличные (критические) значения данного критерия (формула 3.6) из статистических таблиц, делаем вывод о статистической значимости различий в экспериментальной и контрольной группах. Подробный анализ в Приложении 15.

В таблице 3.13 представлены сводные данные по анализу (с помощью *φ**-критерия углового преобразования Фишера) статистической значимости различий результатов в ЭГ и КГ в трех сериях формирующего эксперимента по обучению технологиям защиты информации будущих специалистов финансово-экономической сферы.

Таблица 3.13. φ*-критерий углового преобразования Фишера для выборок формирующего эксперимента

Год, семестр	Выборка	Количество студентов	$\varphi^*_{эмп}$	$\varphi^*_{крит}$ ($p=0.05$)	$\varphi^*_{крит}$ ($p=0.01$)	p	Принимается гипотеза
2019-2020 осенний семестр	ЭГ	5	2,27	**1.64**	2.31	0,011	H_1
	КГ	6					
2019-2020 весенний семестр	ЭГ	7	3,91	1.64	**2.31**	0,000	H_1
	КГ	17					

2020-2021 осенний семестр	ЭГ	10	1,84	**1.64**	2.31	0,033	H_1
	КГ	10					
Итого		55					

Эмпирическое (расчетное) значение φ*-критерия углового преобразования Фишера ($\varphi^*_{эмп}$) сравнивают с критическим значениям: $\varphi^*_{кр} = 1.64$ при p=0,01 и $\varphi^*_{кр} = 2{,}31$ при p=0,05.

По результатам итогового тестирования в осеннем семестре 2019-2020 уч. г. определено, $\varphi^*_{эмп} > \varphi^*_{крит}$ (2,27>1.64). Таким образом, гипотеза H_0 отклоняется, и принимается гипотеза H_1 на уровне значимости p=0.011 о том, что в осеннем семестре 2019-2020 уч. г. доля студентов достигнувших уровня 66 баллов в ЭГ выше, чем в КГ.

По результатам итогового тестирования в весеннем семестре 2019-2020 уч. г. определено, что $\varphi^*_{эмп} > \varphi^*_{крит}$ (3,91>2,31). Таким образом, гипотеза H_0 отклоняется, и принимается гипотеза H_1 на уровне значимости p=0.000 о том, что в весеннем семестре 2019-2020 уч. г. доля студентов набравших более 66 баллов в ЭГ выше, чем в КГ.

По результатам итогового тестирования в осеннем семестре 2020-2021 уч. г. определено, $\varphi^*_{эмп} > \varphi^*_{крит}$ (1,84>1,64). Таким образом, гипотеза H_0 отклоняется, и принимается гипотеза H_1 на уровне значимости p=0.033 о том, что в осеннем семестре 2020-2021 уч. г. доля студентов набравших 66 баллов и более в ЭГ выше, чем в КГ.

Можно сделать вывод, что в каждой серии формирующего эксперимента подтверждается гипотеза H_1, т.к. эмпирические значения φ*-критерия больше критического при p=0,05, и даже больше табличного значения при p=0,01 в весеннем семестре 2019-2020 уч. г. Таким образом, результаты расчетов можно представить следующим образом: уровень обученности в ЭГ статистически значимо выше, чем уровень обученности в КГ на уровне значимости p<0,05 в каждой серии формирующего эксперимента (рис. 3.11).

Рис. 3.11. Границы принятия гипотезы по φ*-критерию в трех сериях формирующего эксперимента

3.4 Выводы к главе 3

Организация и проведение педагогического эксперимента позволили сформулировать следующие выводы:

1. Констатирующий эксперимент продемонстрировал необходимость применения

ИКТ, в том числе интернет-технологий, в процессе изучения университетской дисциплины «Информационная безопасность», подготовив предпосылки для дальнейшего развития педагогической модели и методологии внедрения, ориентированной на интеграцию новых информационных технологий в учебный процесс, с целью повышения качества изучения технологий защиты и безопасности информации в рамках профессиональной подготовки студентов экономико-финансовой сферы, что будет способствовать успешному интегрированию на рынке труда.

2. Формирующий эксперимент, проведенный за 2019-2020 и 2020-2021 учебные года, продемонстрировал эффективность использования ИКТ, в том числе интернет-технологий, при изучении дисциплины «Информационная безопасность». Показано, что, внедряя интерактивные обучающие технологии и стратегии, преподаватель выстраивает эффективные партнерские отношения с обучающимися, помогая им получать знания и развивать свои интеллектуальные способности, умения, навыки, склонности, чувства и эмоции.

3. Проведенный педагогический эксперимент позволил на основе статистического анализа сделать следующие общие выводы:

– продемонстрирована эффективность педагогической модели, ориентированной на использование интерактивных технологий в изучении университетской дисциплины «Информационная безопасность», и методологии внедрения посредством фиксации более эффективных результатов в экспериментальных выборках по сравнению с контрольными выборками;

– в результате проведенного исследования были выявлены различия в уровне обученности студентов в двух группах сравнения. Проанализировав полученные данные, можно сделать вывод, что использование инновационных методов и средств обучения оказывает значительное влияние на уровень обученности студентов и формирование их компетенций в области информационной безопасности;

– доказана рациональность использования информационно-коммуникационных, в том числе и интернет технологий, по сравнению с традиционным способом процесса преподавания – обучения – оценивания;

– эффективность разработанной педагогической модели обучения дисциплине «Информационная безопасность» была подтверждена с помощью таких статистических методов, как U – критерия Манна – Уитни и φ*–критерия углового преобразования Фишера;

– осуществлено сравнение эффективности нескольких вариантов педагогических воздействий. При исследовании среднего значения результатов студентов

по отдельным критериям обученности по дисциплине «Информационная безопасность», установлено, что результаты студентов экспериментальных групп оказались выше результатов студентов контрольных групп по большинству критериев оценивания уровня обученности;

– использование информационно-коммуникационных, в том числе интернет-технологий, способствует повышению результатов освоения критерия обученности, определяющего знание основ информационной безопасности, и повышению уровня сформированности практических навыков по защите компьютерной информации;

– на основе полученных результатов внесены изменения в структуру теоретических и практических работ дисциплины «Информационная безопасность», разработаны лабораторные и практические работы, которые позволяют сформировать навыки в области информационной безопасности для будущих специалистов финансово-экономической сферы, а также дополнительные практические работы, которые позволяют глубже изучить возможности защиты информации с помощью электронно-цифровой подписи.

Эти изменения дали положительные тенденции в повышении уровня обученности студентов, которые подтвердились обработкой результатов итогового тестирования по дисциплине «Информационная безопасность».

ОБЩИЕ ВЫВОДЫ И РЕКОМЕНДАЦИИ

Проведенное теоретико-экспериментальное исследование направлено на создание теоретико-методологической основы процесса изучения технологий защиты информации и информационной безопасности будущими специалистами финансово-экономической сферы с применением интернет-технологий и интерактивных стратегий обучения.

Таким образом, **решаемая научная проблема заключается** в определении теоретико-методологических основ повышения эффективности и качества изучения технологий защиты информации и информационной безопасности с перспективы интернет-технологий и кибернетического подхода, что привело к теоретическому обоснованию и разработке педагогической модели формирования профессиональных компетенций будущих квалифицированных специалистов финансово-экономической сферы, востребованных на рынке труда.

Задачи исследования были выполнены, что способствовало прояснению технологических и методологических аспектов проблемы исследования.

Из анализа полученных результатов можно сделать следующие **выводы**:

1. Проанализированы научные исследования и научная литература, посвященная вопросам обучения информационной безопасности. Изучены нормативно-правовые документы, Доктрины, Стратегии разных стран мира в области информационной безопасности. Информационная безопасность рассмотрена как часть цифровой компетенции. Исследованы Стандарты, учебные планы по обучению информационной безопасности в вузах разных стран мира. Определены рамки изучения дисциплины «Информационная безопасность» будущими специалистами финансово-экономической сферы [19, 70, 73, 79].

2. Разработана педагогическая модель обучения будущих специалистов финансово-экономической сферы с позиций кибернетического подхода с помощью аппарата теории систем и системного анализа. Разработанная педагогическая модель позволяет формировать у будущих специалистов финансово-экономической сферы компетенции в области информационной безопасности с учетом требований государственных образовательных стандартов и рынка труда, потребностям личности в цифровой экономике. Также обеспечивает успешное усвоение дисциплины «Информационная безопасность», повышает уровень обученности студентов, способствует формированию навыков самостоятельного усвоения учебного материала и его практического применения [62, 82].

3. Теоретически обосновали, что для повышения эффективности обучения и формирования практических навыков по дисциплине «Информационная безопасность» будущими специалистами финансово-экономической сферы необходимо:

a) реализовывать содержание обучения в организационных формах, способствующих проявлению познавательной активности и профессиональной направленности студентов, таких как лекции-дискуссии, лекции-конференции, видеолекции, тематическая, групповая дискуссии [158];

b) организовывать самостоятельную внеаудиторную деятельность студентов: проектную деятельность, веб-квест, «устранение цифрового неравенства» [3, 67, 78, 80];

c) применять такие методы мотивации и стимулирования учебно-познавательной деятельности как: балльно-рейтинговая система, подготовка презентаций студентами, участие в студенческих конференциях [16, 20];

d) использовать технологии обучения, способствующие повышению уровня обученности студентов в процессе изучения дисциплине «Информационная безопасность» и расширению опыта использования полученных умений и навыков в личной жизни и будущей профессиональной деятельности [91];

e) для формирования практических навыков использовать лабораторные работы по программным способам защиты информации, с применением различных средств, а также использовать встроенные утилиты операционных систем, современное свободно распространяемое программное обеспечение, такое как drweb Cureit, cCleaner, 7-Zip [69];

f) использовать он-лайн инструменты в процессе преподавания-обучения-оценивания, такие как Joomag, TestMoz, GoogleSites, GoogleForms, необходимые для оперативного представления при необходимости изменения учебно-методических материалов для организации учебного процесса не только в стенах образовательного учреждения, но и за его пределами [16, 18, 72, 81];

g) применять междисциплинарный подход, способствующий выработке новых обобщённых умений, формированию научного и идейно-нравственного мировоззрения; оказывающий влияние на мотивационную сферу, успехи в учебной и трудовой деятельности [159];

h) подчеркивать взаимосвязь информационной безопасности с экономической безопасностью, а также ее отражение на экономических процессах, для понимания значимости получаемых умений и навыков в своей будущей профессиональной деятельности [82].

4. В результате проведенного педагогического эксперимента: (a) доказана эффективность разработанной педагогической модели с помощью математико –

статистических методов: U – критерия Манна – Уитни и φ*–критерия углового преобразования Фишера; (b) установлена прямая зависимость между использованными методами и средствами обучения и повышением уровня обученности студентов по дисциплине «Информационная безопасность»; (c) установлено, что использование информационно-коммуникационных, в том числе интернет-технологий, способствует повышению уровня сформированности практических навыков в области защиты информации; (d) полностью решена проблема исследования по определению теоретических и методологических основ эффективности обучения дисциплине «Информационная безопасность» [63, 75].

5. Усовершенствованы учебно – методические комплексы по дисциплине «Информационная безопасность» и разработаны новые дидактические материалы средствами ИКТ и он-лайн сервисов (методические указания к проведению лабораторных работ, материалы для входного, текущего и итогового контролей, наборы индивидуальных заданий) для реализации педагогической модели, что позволяет повысить эффективность процесса преподавание – обучение – оценивание [17, 18, 61, 68, 69, 71, 72, 74, 77].

6. На основании выше изложенного, предлагаем следующие практические рекомендации:

1. Для преподавателей:

• Использовать усовершенствованные учебно – методические комплексы и новые дидактические материалы, размещенные на он-лайн по дисциплине «Информационная безопасность» для повышения эффективности процесса преподавание – обучение – оценивание.

• Использовать разработанную методологию для повышения эффективности обучения дисциплине «Информационная безопасность».

2. Для авторов учебников и учебных пособий:

• Применять предложенную педагогическую модель в разработке новых учебников и учебных пособий.

• Применять разработанные материалы при изучении практической части дисциплины «Информационная безопасность», а также для входного, текущего и итогового контролей.

3. Для студентов и мастерандов:

• Изучать разработанную педагогическую модель.

• Изучать технологии защиты информации для обеспечения ее безопасности с использованием подхода, основанного на проектах и при формировании практических

навыков использовать по дисциплине «Информационная безопасность» разработанные дидактические он-лайн средствами материалы.

Проведенное исследование открывает новые перспективы изучения технологий защиты информации и информационной безопасности будущими специалистами финансово-экономической сферы посредством внедрения интернет-технологий и интерактивных стратегий обучения. Принимая во внимание вышеизложенные выводы, можно сделать вывод, что затронутые темы являются актуальными и это обусловило выбор темы для всестороннего исследования процесса формирования профессиональных компетенций будущих квалифицированных специалистов для национальной экономики.

Выполненное исследование может быть в дальнейшем углублено в направлении подготовки и развития у будущих специалистов финансово-экономической сферы навыков критического восприятия информации и цифровой этики с перспективы интернет технологий и интерактивных стратегий обучения.

БИБЛИОГРАФИЯ

Правовые акты

1. Закон Республики Молдова об утверждении Концепции информационной безопасности Республики Молдова: № 299 от 21 декабря 2017 года. В: *Monitorul Oficial al Republicii Moldova,* 2018, nr. 48-57, 122.
2. Регламент (ЕС) относительно Агентства Европейского Союза по сетевой и информационной безопасности: № 526/2013 от 21.05.2013. [online]. *Официальный сайт Европейского Союза,* 2021 [citat 23.09.2021]. Доступен: https://eur-lex.europa.eu/eli/reg/2013/526/oj
3. Постановление Парламента Республики Молдова об утверждении Стратегии информационной безопасности Республики Молдова на 2019–2024 годы и Плана действий по ее реализации: №257 от 22.11.2018. В: *Monitorul Oficial al Republicii Moldova*, 2019, nr. 13-21, 80.
4. Постановление Правительства Республики Молдова об утверждении Национальной рамки квалификаций Республики Молдова: nr. 1016 от 23.11.2017. В: *Monitorul Oficial al Republicii Moldova,* 2017, nr. 421-427, 1137.
5. Постановление Правительства Республики Молдова о Национальной стратегии создания информационного общества - "Электронная Молдова": №255 от 09.03.2005. В: *Monitorul Oficial al Republicii Moldova,* 2005, nr. 46-50, 336.
6. Постановление Правительства Республики Молдова о Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы: № 811 от 29.10.2015. В: *Monitorul Oficial al Republicii Moldova,* 2015, nr. 306-310, 905.
7. Приказ Минобрнауки РФ от 12.08.2020 N 954 "Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 38.03.01 Экономика" (Зарегистрировано в Минюсте РФ 25.08.2020 N 59425) – https://minjust.consultant.ru/documents/46969?items=1&page=1
8. *ФГОС ВО по направлениям бакалавриата*. Портал Федеральных государственных образовательных стандартов высшего образования РФ, ©2021 [citat 04.07.2021]. Доступен: https://fgosvo.ru/fgosvo/index/4/88.

Научные источники

9. AFANAS Dorin. Fundamentele strategice privind dezvoltarea conceptului STEAM în cadrul laboratorului „Inteligența Artificială Creativă”. In: *Conferința științifică international „Abordări inter/transdisciplinare în predarea științelor reale, (concept STEAM)” dedicată aniversării a 70 de ani de la nașterea profesorului universitar Anatol Gremalschi, vol.I* . Chișinău, 2021, p. 171-180. ISBN 978-9975-76-357-8.

10. ANDERSON, J. Information security in a multi-user computer environment. In: *Advances in Computers*, vol. 12. New York: Academic Press, 1973, pp. 1-35. (I A1, SFR) DOI: 10.1016/S0065-2458(08)60506-9

11. ANDERSON, R. J. Searching for the Optimum Correlation Attack. In: *Fast Software Encryption*, 1994. pp. 137-143. ISBN 978-3-540-60590-4.

12. ANDERSON, R. Why Information Security is Hard An Economic Perspective. В: *17th Annual Computer Security Applications Conference. December 10-14, 2001. New Orleans, Louisiana.* [online]. 2001 [citat 05.08.2021]. Доступен: https://www.acsac.org/2001/papers/110.pdf

13. ATANASIU, Adrian. *Securitatea Informației.* Vol. 1 (Criptografie). Cluj: Editura INFODATA, 2012. 237 p. ISBN 978-973-1803-16-6.

14. BILIC, E. V. **BOGDANOVA, V. A.**, GRADINARI, O. A. The pedagogical methods and techniques for developing information and communication skills in information disciplines In: *Перший Міжнародний науково-практичний WEB-форум Розбудова єдиного відкритого інформаційного простору освіти впродовж життя, 26–28 березня 2019, Київ-Харків.* Кропивницький, Украина: Вид-во Льотної академії Національного авіаційного університету.Вип.1, 2019, с. 70-71**.**

15. **BOGDANOVA, V.** Metodologia implementării conceptului „eliminarea decalajului digital" în procesul studierii disciplinei „Securitatea Informațională". In: "*International Symposium "Actual Problems of Mathematics and Informatics": dedicated to the 90th birthday of professor Ion Valuţă, november 27-28, 2020, Chişinău*. Chişinău: Tehnica-UTM, 2021, p. 128. ISBN 978-9975-45-677-7.

16. **BOGDANOVA, V.** Применение балльно-рейтинговой системы контроля знаний при изучении дисциплины «Информационная безопасность» студентами экономистами. В: *Conferinţa ştiinţifică cu participare internaţională «Învăţământul superior: tradiţii, valori, perspective», Chişinău, 1 - 2 octombrie 2021*. Chişinău : UST, 2021, vol. 1, pp. 30-36. ISBN 978-9975-76-361-5.

17. **BOGDANOVA, V.,** CHIRIAC, L. Repere didactice privind studierea algoritmilor care țin de autentificare și semnăturile digitale In: *Conferința Republicană a cadrelor didactice*, 1-2 martie 2019. Chișinău: UST, 2019. p. 174-179. ISBN 978-9975-76-271-7.

18. **BOGDANOVA, V.,** CHIRIAC, L. The digital publishing platform joomag for organizing independent work of students In: *Розбудова єдиного відкритого інформаційного простору освіти впродовж життя (Forum-SOIS, 2020), II Міжнародний науково-практичний WEB-форум, 25-27 march 2020*. Харьков, Украина: «Мадрид», 2020, с. 201-202.

19. BOGDANOVA, V., CHIRIAC, L. The potential of the discipline "Information Security"

in the digital competence formation in training future economists. In: *Conference on Applied and Industrial Mathematics. CAIM 2019, Targoviste, September 19-22, 2019*. Chişinău: UST, 2019. p.14-17. ISBN 978-9975-76-282-3.

20. **BOGDANOVA, V**., KHMELNITSKAYA, E., CHIRIAC, L. Some aspects about the application of distance technologies in professional education. In: *Acta Et Commentationes. Ştiinţe ale Educaţiei.* 2020, Nr. 2(20), pp. 52-57. ISSN 1857-0623.

21. CABAC, G. Individuaizarie formării în medii digitate prin construiria trazeelor individuale de instruire. In: *Formaria universitară în medii digitale: cercetări teoretico-experimentale*. Bălţi, 2015, p.197-236.

22. CANŢER, N. *Didactica predării informaticii în învăţământul universitar: (Suport pentru prilegeri).* Chişinău: CEP USM, 2007. 65 p. ISBN 978-9975-70-470-0.

23. CARA, Angela, GREMALSCHI, Anatol, ACHIRI, Ion. Integrarea Educaţiei financiare în curricula naţionale. In: *Univers Pedagogic*. 2016, nr. 2(50), pp. 3-9. ISSN 1811-5470.

24. CHIRIAC, L., DANILOV, A., **BOGDANOVA**, V. Utilizarea conceptelor din teoria numerelor in elaborarea algoritmilor criptografici asimetrici In: *Învăţământ superior: tradiţii, valori, perspective, Conferinţa ştiinţifica naţionala cu participare internaţională, vol.I, 29-30 septembrie 2020*. Chişinău: UST, 2020, pp. 239-247. ISBN 978-9975-76-311-0.

25. CHIRIAC, L., GLOBA, A. Studierea informaticii în învăţământul preuniversitar prin prisma metodelor și tehnicilor moderne de programare. In: *Studia Universitatis. Seria Ştiinţe ale educaţiei*. 2016, nr. 5(95). pp. 231-241. ISSN: 1857-2103.

26. CRISTEA, S. *Dictionar de Termeni Pedagogici*. Bucureşti: Editura didactică şl pedagogică. 1998. 312 p. ISBN 973-30-5130-6.

27. CRISTEA, S. Instruirea prin proiecte. În: *Didactica Pro*. 2018, nr. 1(107), p. 57-60. ISSN 1810-6455.

28. DAIMI, K., FRANCIA, G. *Innovations in Cybersecurity Education*. Springer, 2020, 388 p. ISBN 978-3-030-50243-0.

29. DODGE, B. Some Thoughts About WebQuests. URL: http://webquest.sdsu.edu/about_webquests.html (дата обращения: 25/09/2018).

30. GĂBUDEANU, L. Propunere pentru abordări practice în educația privind securitatea informației. In: *Securitatea cibernetică - Provocări și perspective în educație*, ROMÂNIA, 2020. p.183-190. ISBN 978-606-11-7675-5.

31. GREMALSCHI, A. ş.a. Lecţii interactive pentru instruirea la distanţa în domeniul tehnologiei informaţiei şi a comunicaţiilor. In: *„Învăţământul universitar din Republica Moldova la 80 de ani", conf. şt. internaţ. Vol. 2: Probleme actuale ale didacticii matematicii, informaticii şi fizicii*. Chişinău: Univ de Stat din Tiraspol, 2010, pp. 219–230.

32. HELMBRECHT, U. Cybersecurity from a University Perspective In: *Securitatea cibernetică - Provocări şi perspective în educaţie*, ROMÂNIA, 2020. p.29-38. ISBN 978-606-11-7675-5.

33. KAHN, D. *Codebreakers. The story of Secret Writing*. New York: Macmillan, 1967, 473 c.

34. KILPATRICK, W. H. *The Project Method. Teachers College Record,* 1918. 320 p.

35. LEEUW, K. M., BERGSTRA, J. The History of Information Security: A Comprehensive Handbook. Amsterdam: Elsevier, 2007, 900 p. ISBN 978-0-444-51608-4.

36. MIHAI, I. C. *Securitatea informaţiilor*. Craiova: Editura Sitech, 2012. p. 317. ISBN 978-606-11-29203-4.

37. MIHAI, I.-C., CIUCHI, C., PETRICĂ, G.-M. *Provocări actuale în domeniul securităţii cibernetice - impact și contribuția României în domeniu.* București, 2018. 89 p. ISBN online 978-606-8202-60-0.

38. PERIZAT, B., SEITKAZYA. A Web-Quest as a Teaching and Learning Tool IEJME. In: *Mathematics Education*, 2016, Vol. 11, No 10, Ankara: Turkey, p. 3537-3549.

39. PLOTEANU, N. Matricea infractorilor computaţionali . In: *Anale ştiinţifice ale Academiei „Ştefan cel Mare" a MAIRM: ştiinţe juridice.* 2003, nr. IV, pp. 253-260. ISSN 1857-0976.

40. POPA, S. E. *Securitatea sistemelor informatice. Note de curs şi aplicaţii pentru studenţii Facultăţii de Inginerie*. Bacău: Editura Alma Mater, 2007. 136 p. ISBN: 978-973-1833-21-7.

41. SALTZER, J. H. SCHROEDER, M. D. The protection of information in computer systems. In *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278-1308, Sept. 1975, DOI: 10.1109/PROC.1975.9939 URL: web.mit.edu/Saltzer/www/publications/protection/index.html

42. SARCINSCHI, A. *Vulnerabilitate, risc, ameninţare. Securitatea ca reprezentare psihosocială*. Bucureşti: Editura Militară, 2009. p. 248. ISBN: 978-973-32-0739-9.

43. SILISTRARU, Nicolae. GOLUBIŢCHI, Silvia *Pedagogia învăţământului superior: Ghid metodologic*. Chişinău: UST, 2013. 192 p. ISBN 978-9975-76-102-4.

44. SKINNER, B. F. *The Technology of Teaching*. New York: Appleton-Century-Crofts.1968, 255 c.

45. SMITH, R. E. *Elementary Information Security*. Burlington: Jones & Bartlett Learning, 2013. 892 p. ISBN 978-1-4496-4820-6.

46. SPAFFORD, E. James P. Anderson: An Information Security Pioneer. In: *IEEE Security and Privacy Magazine.* February 2008. 6 (1). p. 9 DOI:10.1109/MSP.2008.15

47. STANCIU, V., TINCA, A. *Securitatea informației. Principii si bune practici*. Ediția a doua. Bucuresti : Editura ASE, 2015. 232 p. ISBN 978-606-505-902-3.

48. UDROIU, M. POPA, C. *Securitatea informaţiilor în societatea informaţională*.

Bucureşti: Editura Universitară, 2010. p. 402. ISBN: 978-973-749-831-1.

49. ZGUREANU, A. *Securitatea informaţională şi metode de criptare bazate pe mulţimi de relaţii multi-are*: tz. de doct. în ştiinţe fizico-matematice. Chişinău, 2011. 160 p.

50. АБИССОВА, М. А. *Сервисы обучения информационной безопасности в теории и методике обучения информатике студентов гуманитарных и социально-экономических специальностей*: дис. . канд. пед. наук. Санкт-Петербург, 2006. 214 с.

51. АБИССОВА, М. А., ФОКИН, Р. Р. Сервисы обучения информационной безопасности в курсе информатики для студентов гуманитарных и социально-экономических специальностей. В: *Педагогическая информатика*. *Специальный выпуск*. 2006. № 6. с. 115–117.

52. АЙЗИКОВА, Л. В. К вопросу об обучении на протяжении жизни В: *Наука о человеке: гуманитарные исследования*. 2012, №1 (9), с. 35-41.

53. АКТАЕВА, А., БАЙКЕНОВ, А., ГАЛИЕВА, Н., АСАНОВА, К., БАЙМАН, Г., ШАТЕНОВА, Г. Квантовая информация: методы защиты информации. В: *Современные информационные технологии и ИТ-образование*. Том 12. 2016, № 2, с. 6-14. ISSN 2411-1473.

54. АЛТУФЬЕВА, А. А. *Методические основы обучения информационной безопасности на базе телекоммуникационных ресурсов сети Интернет*: автореф. дис. канд. пед. наук. Санкт-Петербург, 2008. 20 с.

55. АНУРЬЕВА, М.С. Современная система образования в области информационной безопасности в Российской Федерации В: *Вестник Тамбовского университета*. Серия Гуманитарные науки. 2018. Т. 23, № 173. с.111-120. ISSN 1810-0201.

56. АРСЕНТЬЕВ, М. В. К вопросу о понятии «информационная безопасность». В*: Информационное общество*. 1997, № 4-6. с. 48-50.

57. АСМОЛОВ, А. Г. *Психология личности: культурно-историческое понимание развития человека*. 3-е изд. Москва: Смысл: Издательский центр «Академия», 2007. 528 с. ISBN 978-5-89357-221-6.

58. АТКИНСОН, Р. Л., АТКИНСОН, Р. С., СМИТ, Э. Е., БЕМ, Д. Дж. *Введение в психологию*. 13 изд. 2003. 713 с. ISBN 5-93878-097-7.

59. БИМ-БАД, Б.М. М.М. *Педагогический энциклопедический словарь.* 3-е изд. Москва: Большая Российская энциклопедия, 2009. 527 с. ISBN 978-5-85270-230-2.

60. БЛИНКОВ, Ю.В. *Основы теории информационных процессов и систем*. Пенза: ПГУАС, 2011. 184 с. ISBN 978-5-9282-0725-0.

61. **БОГДАНОВА, В. А**. Веб-квест технология в обучении информационной безопасности студентов экономического профиля In: *Применение современных образовательных информационных технологий в развитии профессиональных*

компетенций студентов высшей школы, 7-8 декабря, 2018. Бельцы: Profadapt, 2018, с. 144-148. ISBN 978-9975-3276-0-2.

62. **БОГДАНОВА, В. А**. Информационно-кибернетический подход к проектированию педагогического эксперимента In: *Revista de Stiinţe Socioumane*. 2021, Nr. 2 (48), с. 112-125. ISSN 1857-0119.

63. **БОГДАНОВА, В. А.** Методология обработки педагогической информации с помощью критериев ϕ*-углового преобразования Фишера и Манна-Уитни. In: *Revista Univers Pedagogic*. 2021, Nr.3(71), с. 56-63. ISSN 1811-5470.

64. **БОГДАНОВА**, **В. А.** Профессиональные ценности современного педагога. In: *Перспективы и проблемы интеграции в Европейское исследовательское образовательное пространство*. *Межд. науч. конф. 7 июня 2018*. Кагул: Centrografic, 2018, pp. 25-28. ISBN 978-9975-88-040-4.

65. **БОГДАНОВА**, В. А., БЕШЛЯГА, К. Ю., ПУШКАРЕВА, Д. М. Из опыта оценки уровня цифровой грамотности в преодолении цифрового неравенства. В: *Научно-практическая конференция «Экономическая кибернетика: теория, практика и направления развития*». *Одесский национальный политехнический университет. 24-25 ноября 2020.* Одеса**,** Украина: ОНПУ, 2020, с. 38-41.

66. **БОГДАНОВА, В. А.,** ГОРАШ, И. С. SWOT-анализ процесса поиска и подбора персонала с применение цифрового следа. In: *Науково-практична інтернет-конференція «Економічна кібернетика: теорія, практика та напрямки розвитку», кафедри Економічної кібернетики та інформаційних технологій Одеського національного політехнічного університету.Одеський національний політехнічний університет, 27-28 листопада 2019*. Одеса, Украина: ОНПУ, 2019, с. 18-21.

67. **БОГДАНОВА, В. А.,** ДАРИЕНКО, М. С. Возможности интеграции Web-квест технологии на этапе обобщения и систематизации знаний обучающихся. In: *Общекультурные и естественнонаучные аспекты образования в интересах устойчивого развития, 25 ноября – 3 декабря 2018.* Арзамас, Россия: Арзамасский филиал ННГУ, 2018. с.134-138. ISBN 978-5-6040222-9-0.

68. **БОГДАНОВА,** В. А., КИРИЯК, Л. Л. Проектирование практического занятия по теме «Алгоритмы хеширования и электронно-цифровой подписи» для студентов гуманитарного профиля. In*: Материалы Национальной научной конференции с международным участием «Высшее образование: традиции, ценности, перспективы», 28-29 сентября 2018 года, Т.1.* Кишинэу: UST Printing, 2018, с. 134-138. ISBN 978-9975-76-252-6.

69. **БОГДАНОВА, В. А**., КИРИЯК, Л. Л. Внедрение информационных технологий в

процессе изучения курса «Защита компьютерной информации» In: *4-ая Конференция математического сообщества Р. Молдова, посвященная столетию со дня рождения Владимира Андрунакевича (1917-1997), CMSM, Материалы по дидактике 4, июнь 28- июль 2, 2017*. Кишинэу: UST, 2017, pp. 42-49. ISBN 978-9975-76-203-8.

70. **БОГДАНОВА, В. А**., КИРИЯК, Л. Л. Методическая система обучения дисциплины «Защита компьютерной информации» студентам гуманитарного профиля. In: *Acta Et Commentationes. Педагогические науки.* 2018, № 2(13), pp. 50-61. ISSN 1857-0623.

71. **БОГДАНОВА, В. А.**, КИРИЯК, Л. Л. Организация текущей работы студентов экономического профиля при обучении дисциплине «Защита компьютерной информации» In: *Актуальные проблемы дидактики фундаментальных наук, Научно-дидактической конференции с международным участием II, посвященная 80-летию профессора Илие Лупу, 11-12 мая 2018, Т.1*. Кишинэу: UST, 2018, pp. 125-130. ISBN 978-9975-76-237-3.

72. **БОГДАНОВА, В. А.,** КИРИЯК, Л. Л. Особенности проектирования веб-квеста «Информационная безопасность экономистов». In: *Conferința științifica națională cu participare internaţională „Învăţământ Superior: Tradiţii, Valori, Perspective". Didactica Ştiinţelor. 27 – 28 septembrie, 2019.* Chişinău: UST, 2019, pp. 127-131. ISBN 978-9975-76-284-7.

73. БОГДАНОВА, В. А., КИРИЯК, Л. Л. Особенности процесса преподавания дисциплины «Защита компьютерной информации» студентам экономического профиля подготовки In: *III Міжнародної науково-практичної конференції Інформаційна безпека та комп'ютерні технології, 19-20 квітня 2018*. Кропивницький, Украина: ЦНТУ, 2018. с. 36-39.

74. **БОГДАНОВА, В. А**., КИРИЯК, Л. Л. Проектирование занятия по информационной безопасности для студентов гуманитарного профиля. In: *26-ой Международной конференция Прикладной и промышленной математики CAIM 2018: Секция образование, 20-23 сентября, 2018*. Кишинэу: Изд-во Тираспольского Государственного университета, 2018, с. 65-72. ISBN 978-9975-76-247-2.

75. **БОГДАНОВА, В. А**., КИРИЯК, Л. Л. Проектирование педагогического эксперимента по обучению защите информации экономистов. In: *Materialele Conferintei Republicane a Cadrelor Didactice, 28-29 februarie 2020, Vol 1*. Chişinău: UST, 2020, pp. 236-242. ISBN 978-9975-76-305-9.

76. **БОГДАНОВА, В. А.**, ХМЕЛЬНИЦКАЯ, Е. А., БАЛАН, И. Ю. Вызовы образования в преодолении цифрового неравенства В: *Научно-практическая интернет-конференция «Экономическая кибернетика: теория, практика и направления развития». Одесский национальный политехнический университет. 24-25 ноября 2021.* Одеса**,** Украина: ОНПУ, 2021, с. 42-46.

77. **БОГДАНОВА, В. А.,** ЦЫНЦАРЬ, А. Л. Использование квест-технологии в

образовательном процессе студентов БПФ In: *Экономическая психология инновационного менеджмента, X Всероссийская научно-практическая конференция с международным участием, 13 декабря 2018, Брянск*. Брянск, Россия: БГТУ, 2019, с.132-140. ISBN 978-5-6043654-9-6.

78. **БОГДАНОВА,** В. Реализация концепции «Устранение цифрового неравенства» в рамках дисциплины «Информационная Безопасность» при обучении экономистов в ВУЗе In: *Învăţământ superior: tradiţii, valori, perspective, Conferinţa ştiinţifica naţionala cu participare internaţională, vol.I, 29-30 septembrie 2020.* Chişinău: UST, 2020, pp.357-361. ISBN 978-9975-76-311-0.

79. БОГДАНОВА, В., ГРАДИНАРЬ, О., БИЛИК, Е. Цифровая компетенция как часть профессиональной компетенции будущего экономиста. In: *Utilizarea tehnologiilor educaţionale şi informaţionale moderne pentru formarea competenţelor profesionale ale absolvenţilor instituţiilor de învăţământ superior, Conferinţa ştiinţifico-practice cu participare international, 6-7 decembrie 2019*. Bălți: USARB, pp. 224-228. ISBN 978-9975-3369-3-2.

80. **БОГДАНОВА, В.**, ГРАДИНАРЬ, О., ХМЕЛЬНИЦКАЯ, Е. Steam-подход в реализации учебного проекта «женщины в IT и кибербезопасности». В: *Conferința științifică internațională „Abordări inter/transdisciplinare în predarea științelor reale, (concept STEAM)" dedicată aniversării a 70 de ani de la naşterea profesorului universitar Anatol Gremalschi. Chișinău, 29 - 30 octombrie 2021*. Chişinău : UST, 2021, с. 343 -343. ISBN 978-9975-76-357-8.

81. **БОГДАНОВА, В**., КИРИЯК, Л. Особенности применения ментальных карт с перспективы STEAM в обучении будущих экономистов основам информационной безопасности. В: *Conferința științifică internațională „Abordări inter/transdisciplinare în predarea științelor reale, (concept STEAM)" dedicată aniversării a 70 de ani de la naşterea profesorului universitar Anatol Gremalschi. Chișinău, 29 - 30 octombrie 2021*. Chişinău : UST, 2021, с. 336 -339. ISBN 978-9975-76-357-8.

82. **БОГДАНОВА, В**., КИРИЯК, Л. Системный подход в обучении информационной безопасности будущих экономистов. In: *Materialele Conferinţei Republicane a Cadrelor Didactice, 27-28 februarie 2021*, Chișinău: Tipogr. UST, 2021, pp. 180-184. ISBN 978-9975-76-324-0.

83. БОЯРОВ, Е. Н. *Концептуальные подходы к обучению специалиста информационной безопасности в университете:* дис. канд. пед. наук. Санкт-Петербург, 2008. 151 с.

84. ВЕЛИКОВА, Т. Использование платформы дистанционного обучения при изучении дисциплины «Информационная безопасность». In: *Teoria şi practica administrării publice*. 20 mai 2013, Chișinău. Chișinău, Republica Moldova: Academia de Administrare

Publică, 2013, pp. 449-452. ISBN 978-9975-4241-5-8.

85. ВИНЕР, Н. *Кибернетика или управление и связь в животном и машине,* 2-е изд. Москва: Советское радио, 1968, 328 с.

86. ВОЛКОВА, В. Н., ЕМЕЛЬЯНОВ, А. А. и др. *Теория систем и системный анализ в управлении организациями: Справочник*. Москва: Финансы и статистика, 2006. 848 с. ISBN 5-279-02933-5.

87. ГЛОТОВА, Е.Е. Требования работодателей к выпускникам вузов: компетентностный подход. В: *Человек и образование*. 2014, № 4 (41). с.185-187. ISSN 1815-7041.

88. ГОРАШ, И., **БОГДАНОВА,** В., ДАРИЕНКО, М. Цифровая тень и цифровой след как угроза информационной безопасности. In: *Utilizarea tehnologiilor educaţionale şi informaţionale moderne pentru formarea competenţelor profesionale ale absolvenţilor instituţiilor de învăţământ superior, Conferinţa ştiinţifico-practice cu participare international, 6-7 decembrie 2019*. Bălți: USARB, pp. 127-131. ISBN 978-9975-3369-3-2.

89. ГОРБУНОВ, А. И. Сущность и содержание профессиональной компетентности экономистов в области информационной безопасности. В: *Мир науки, культуры, образования*. № 6 (31) 2011. с.155-158. ISSN 1991-5497.

90. ГОРБУНОВА, В.В. *Экспериментальная психология в схемах и таблицах*. Киев: ВД «Професіонал, 208. с. ISBN 978-966-370-067-0.

91. ГРАДИНАРЬ, О. И., БИЛИК, Е. А., **БОГДАНОВА, В. А.** Приёмы, методы и технологии обучения, направленные на формирование информационной и коммуникативной компетенции с учетом требований информационной безопасности. In: *Матеріали Міжнародної науково-практичної інтернет-конференції «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації*. *Вип. 44.* Переяслав-Хмельницький, Украина: 2019, с. 159-161.

92. ГРОМОВ, Ю. Ю., ДИДРИХ, В. Е., ИВАНОВА, О. Г., ОДНОЛЬКО, В. Г. *Теория информационных процессов и систем*. Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2014. 172 с. ISBN 978-5-8265-1352-1.

93. ГУБЛЕР, Е. В. *Вычислительные методы анализа и распознавания патологических последствий*. Ленинград: Медицина, 1978. 295 с.

94. ГУБСКИЙ, Е.Ф., КОРАБЛЕВА, Г.В., ЛУТЧЕНКО, В.А. *Краткая философская энциклопедия*. Москва: Прогресс - Энциклопедия, 1994. 576с. ISBN 5-01-004135-9.

95. ДАУТОВА, О. Б., ИВАНЬШИНА, Е. В., ИВАШЕДКИНА, О. А., КАЗАЧКОВА, Т. Б., КРЫЛОВА, О. Н., МУШТАВИНСКАЯ, И. В. *Современные педагогические технологии*

основной школы в условиях ФГОС. Санкт-Петербург: КАРО, 2015. 176 с. ISBN 978-5-9925-0890-1.

96. ДЕМЕНТЬЕВ, С. А. Анализ информационной безопасности современного общества: от дисциплинарных методологических подходов к трансдисциплинарному. В: *Общество и право*. 2017, №4 (62), с.249-253. ISSN 1727-4125.

97. ДИМОВ, Е. Д. *Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования*, дис. канд. пед. наук. Москва, 2013. 181с.

98. ЕВСЕЕВА, Ю. И. Программная кибернетика: современное состояние и проблемы. В: *Известия высших учебных заведений. Поволжский регион. Технические на*уки. 2017, № 3 (43), с. 48–59. ISSN 2072-3059.

99. ЗАГВЯЗИНСКИЙ, В. И., АТАХАНОВ, Р. *Методология и методы психолого-педагогического исследования*. 2-е изд. Москва: Издательский центр «Академия», 2005. 208 с. ISBN 5-7695-2146-5.

100. ЗАГОРСКИЙ, А. В., РОМАШКИНА, Н. П. *Угрозы информационной безопасности в кризисах и конфликтах XXI века.* Москва: ИМЭМО РАН, 2015. 151 с. ISBN 978-5-9535-0450-8.

101. ЗИМНЯЯ, И. А. *Педагогическая психология*. 2-е изд. Москва: Логос, 2001. 208 с. ISBN 5-88439-097-1.

102. ИВАНОВ, И. В. *Теория информационных процессов и систем.* 3-е изд. Москва: Издательство Юрайт, 2018. 228 с. 978-5-534-05705-8.

103. ИВЧЕНКО, Ю. С. *Статистика*. Москва: РИОР:ИНФРА-М, 2011. 375 с. ISBN 978-5-369-00636-8

104. КАРАСЕВ, П. А. Стратегия информационной (кибер) безопасности США в XXI веке В: *Вестник Московского Университета. Серия 12: Политические науки*. 2013, № 2, с. 82-102. ISSN 0868-4871.

105. КАШИНА, О. А. О реализации общих принципов кибернетики в инновационном развитии инженерного вуз. В: *Образовательные технологии и общество*. 2018, №3 (Т.21), с. 284-289. ISSN 1436-4522.

106. КЕФЕЛИ, И. Ф. ЮСУПОВА, Р. М. *Информационно-психологическая и когнитивная безопасность.* Санкт-Петербург: ИД «Петрополис», 2017. 300 с. ISBN 978-5-9676-0895-7.

107. КНИГИН А. Н. Междисциплинарность: основная проблема. В: *Вестник Томского государственного университета. Философия. Социология. Политология*. 2008, №3(4), с.14-20. ISSN 2311-2395.

108. КОНОВАЛОВА, М.Д. *Экспериментальная психология: конспект лекций.* Москва: Высшее образование, 2009. 180 с. ISBN 5-9692-0082-4.

109. КОРНЕЕВ, И. К., СТЕПАНОВ, Е. А. *Защита информации в офисе*. Москва: ТК Велби, Изд-во Проспект, 2008. 336 с. ISBN 978-5-482-01976-4.

110. КРАЕВСКИЙ, В. В. *Методология педагогического исследования.* Самара: СамГПИ. 1994. 165 с. ISBN 5-8428-0038-1.

111. КУЗНЕЦОВ, М.В., СИМДЯНОВ, И. В. *Социальная инженерия и социальные хакеры*. Санкт-Петербург: БХВ-Петербург, 2007. 368 с. ISBN 5-94157-929-2.

112. КУРИЛО, А. П., ЗЕФИРОВ, С. П., ГОЛОВАНОВ, В. Б. *Аудит информационной безопасности*. Москва: Издательская группа «БДЦ-пресс», 2006. 304 с. ISBN 5-93306-100-X.

113. КУРИЛО, А. П., МИЛОСЛАВСКАЯ, Н. Г., СЕНАТОРОВ, М. Ю., ТОЛСТОЙ, А. И. *Основы управления информационной безопасностью.* 2-е изд. Москва: Горячая линия-Телеком, 2014. 244 с. ISBN 978-5-9912-0361-6.

114. КЭМПБЕЛЛ, Д. *Модели экспериментов в социальной психологии и прикладных исследованиях*. Москва: Прогресс, 1980. 390 с.

115. ЛАКИН, Г. Ф. *Биометрия*. Москва: Высшая Школа, 1990, 352 с. ISBN 5-06-000471-6.

116. ЛАМИНИНА, О. Г. Возможности социальной инженерии в информационных технологиях. В: *Гуманитарные, социально-экономические и общественные науки.* 2017, №2. ISSN 2220-2404.

117. ЛОМАСКО, П. С. *Методическая система подготовки учителя информатики в области информационной безопасности*: автореф. дис. канд. пед. наук. Красноярск, 2009. 25 с.

118. МАЙЕР, Р. В. *Кибернетическая педагогика: имитационное моделирование процесса обучения:* монография. Глазов: Глазов. гос. пед. ин-т, 2014. 141 с. ISBN 978-5-93008-176-3.

119. МАЛЫХ, Т.А. *Педагогические условия развития информационной безопасности младшего школьника:* дис.канд. пед. наук. Иркутск, 2008. 168 с.

120. МАЛЮК, А. А., ПАЗИН, С. В., ПОГОЖИН, Н. С. *Введение в защиту информации в автоматизированных системах*. Москва: Горячая линия-Телеком, 2001. 148 с. ISBN 5-93517-062-0.

121. МАРУНИЧ, Н., **БОГДАНОВА, В.** Совершенствование методики преподавания информатики в условиях новой реальности In: *Acta et commentationes. Ştiinţe ale Educaţiei*. 2021, nr. 1(23), pp. 72-77. ISSN 1857-0623.

122. МАТВЕЕВ, Н.А. *Педагогическая модель развития компетентности в области информационно - психологической безопасности у курсантов вузов ГПС МЧС* России: автореф. дис. канд. пед. наук. Санкт-Петербург, 2011. 22 с.

123. МЕЛЬНИКОВ, В. П., КЛЕЙМЕНОВ, С. А., ПЕТРАКОВ, А. М. *Информационная безопасность и защита информации*. 3-е изд. Москва: «Академия», 2008. 336 с. ISBN 978-5-7695-4884-0.

124. МЕШКОВА, Л. М. Сущность и структурно-содержательные компоненты активизации учебно-познавательной деятельности студентов технических вузов. В: *Вестник Челябинского государственного педагогического университета,* 2010, №, с.119-125. МИТНИК, К. *Искусство быть невидимым: как сохранить приватность в эпоху Big Data*. Москва: Эксмо, 2019. 464 с. ISBN 978-5-04-094446-0.

125. МИХАЛЕВИЧ, Е. А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность В: *Вестник Российского университета дружбы народов. Серия: Политология*, 2021, 23(2), 254–264. ISSN 2313-1446.

126. НАПАЛКОВ, С. В. *Тематические образовательные Web-квесты как средство развития познавательной самостоятельности учащихся при обучении алгебре в основной школе*. Автореф. дис. ... канд. пед. наук. Саранск, 2013. 26 с.

127. НИКОДИМОВ, И. Ю. Современные проблемы теории информационного права. В: *Вестник Московского государственного лингвистического университета. Образование и педагогические науки*». 2016, №2 (766), с. 105-117. ISSN 2500-3488.

128. НОВИКОВ, Д.А. *Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития*. Москва: ЛЕНАНД, 2016. 160 с. ISBN 978-5-9710-2549-8.

129. ОЖЕГОВ, С.И., ШВЕДОВА, Н. Ю. *Толковый русский словарь русского языка 80 000 слов и фразеологических выражений*. 4-е изд. Москва: ООО «А ТЕМП», 2006. 944 с. ISBN 978-5-9900358-6-7.

130. ОХРИМЕНКО, С. А., СКЛИФОС, К. Ф. Информационная безопасность для экономистов [online]. Лаборатория Информационной Безопасности [citat 18.06.2021]. Доступен: http://security.ase.md/publ/ru/pubru106/o_s.html

131. ПЛАТОНОВ, В. В. *Программно-аппаратные средства защиты информации*. Москва: Издательский центр «Академия», 2013. 336 с. ISBN 978-5-7695-9327-7.

132. ПЛАТОНОВА, Р. И. Моделирование в научно – педагогических исследованиях. В: *Azimuth of Scientific Research: Pedagogy and Psych*ology. 2017, Т. 6, № 3(20), с. 190-193. ISSN 2309-1754.

133. ПОДЛАСЫЙ, И. П. *Педагогика: Теория и технологии обучения.* Москва: Гуманитар., изд. центр ВЛАДОС, 2007. 575 с. ISBN 978-5-691-01553-3.

134. ПОЛАТ, Е. С. *Новые педагогические и информационные технологии в системе образования*. Москва: Издательский центр «Академия». 2003. 272 с. ISBN 5-7695-0811-6.

135. ПОЛЯКОВ В.П., РОМАНЕНКО Ю.А. Педагогическое сопровождение вопросов информационной безопасности личности в отечественном образовании. В: *Труды Международного симпозиума «Надежность и качество». 2018, том 1, с. 64-67. ISSN 2220-6418.*

136. ПОЛЯКОВ, В. П. *Методическая система обучения информационной безопасности студентов вузов*: дис. ... д-ра пед. наук. Н. Новгород, 2006. 538 с.

137. ПОЛЯКОВ, В. П. О системе обучения студентов основам информационной безопасности. В: *Вестник ФА.* 2006, № 3 (39), с. 125-136.

138. ПОЛЯКОВА, Т. А., СТРЕЛЬЦОВ, А. А. *Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры*. Москва: Юрайт, 2016. 325 с. ISBN 978-5-9916-6799-9.

139. ПОЛЯНИНА, А. К. *Управление информационной безопасностью детей*: дис. ... д-ра соц. наук. Н. Новгород, 2022. 344 с.

140. ПОПОВА, С. В., ФЕДОРИНОВ, В. Е. Экономические аспекты доктрины информационной безопасности. В: *Воздушно-космические силы. Теория и практика*. 2018, № 5 (5), с.17-24. ISSN 2500-4352.

141. РАССОЛОВ, И. М. Правовое регулирование в информационной сфере. В: *Актуальные проблемы российского права*. 2016, № 4(65), с. 92-96. ISSN 1994-1471.

142. РОМАНОВ, А. А. Становление экспериментальной педагогики в Германии (к 150-летию со дня рождения В. А. Лая и Э. Мёймана). В: *Историко-педагогический журнал*. 2012, № 4. с. 122-138. ISSN 2304-1242.

143. РОМАНЦЕВ, Ю. В., ТИМОФЕЕВ, П. А., ШАНЬГИН, В. Ф. *Защита информации в компьютерных сетях*. Москва: Радио и связь. 2001. 375 с. ISBN 5-256-01518-4.

144. РОМАШКИНА, Н. ЗАДРЕМАЙЛОВА, В. Эволюция политики КНР в области информационной безопасности В: *Пути к миру и безопасности*. 2020, № 1(58), с. 122-138. ISSN 2307-1494.

145. САДОВСКИЙ, В. Н. Основания общей теории систем. Москва: Наука, 1974, 280 с.

146. СЕРЕБРЯНИК, Е.Э. *Формирование информационно–личностной безопасности учащихся основной школы*: дис. ... канд. пед. наук. Калининград, 2011. 183 с.

147. СИДЕНКО, А.С., ХМЕЛЕВА, В. С. Педагогический эксперимент: понятие и этапы деятельности. В: *Эксперимент и инновации в школе*. 2008, №2, с.21-25.

148. СИДОРЕНКО, Е.В. *Методы математической обработки в психологии*. Санкт-Петербург: ООО «Речь», 2000. 350с. ISBN 5-9268-0010-2.

149. СИНИЦЫН, Д.С. *Психолого–педагогические условия обучения информационно-психологической безопасности подростков*: дис. ... канд. пед. наук. Санкт-Петербург,

2005. 169 с.

150. СОБОЛЕВА Т.А. *История шифровального дела в России*. Москва: ОМА-ПРЕСС-Образование, 2002. 511 с. ISBN 5-224-03634-8.

151. СТОУНЬЕР, Т. Информационное богатство: профиль постиндустриальной экономики. В: *Новая технократическая волна на Западе*. Москва: Знание, 1986. с. 392 – 409.

152. ТАНОВА, Э. В. *Формирование компетентности в области защиты информации у школьников в процессе обучения информатике:* автореф. дис. канд. пед. наук. Екатеринбург, 2005, 2012. 23 с.

153. ТРЕТЬЯКОВА, Е. М. Организация самостоятельной работы студентов с применением новых информационных технологий. В: *Балтийский гуманитарный журнал*. 2016, Т. 5. № 4(17), с. 329-333. ISSN 2311-0066.

154. УРБАХ, В. Ю. *Статистический анализ в биологических и медицинских исследованиях*. Москва: Медицина, 1975. 297 с.

155. ФЕДИНСКИЙ, Ю.И. *Большой толковый словарь официальных терминов: Более 8000 терминов*. Москва: ООО «Издательство Астрель»: ООО «Издательство АСТ, ООО «Транзиткнига», 2004. 1165 с. ISBN 5-17-020421-3.

156. ФЕДОСЮК, Я. В. Закономерности и принципы кибернетики как теоретико-методологическая основа формирования управленческих команд. В: *Сетевой научно-практический журнал Научный результат. Социология и управление.* 2015, №3, с. 89-92. ISSN 2408-9338.

157. ФЕДОТОВА, Г.А. *Методология и методика психолого-педагогических исследований*. Великий Новгород: НовГУ. 2010. 114 с.

158. ЦЫНЦАРЬ, А. Л., **БОГДАНОВА, В. А**., ГРАДИНАРЬ, О. А., БИЛИК, Е. В. Methods of improving information and communicative competence in information disciplines taking into account information security requirements. In: *Материалы XXIV Международной научно-методической конференции «Управління якістю підготовки фахівців», 18-19 квітня 2019 р*. Одеса, Украина. с. 10-11.

159. ЦЫНЦАРЬ, А. Л., **БОГДАНОВА, В. А.,** РУСНАК, И. М. Влияние квест-технологии на формирование междисциплинарных связей в подготовке бакалавров. In: *Мир университетской науки: культура, образование*. 2019, №8, с. 49-54. ISSN: 1995-1140.

160. ЧЕЛНОКОВ, В. В. *Психологические аспекты обеспечения Информационной безопасности*. Екатеринбург: УрГУ, 2008. 47 с.

161. ЧИБАКОВ, А.С. Кибернетический подход в обучении: историко-эволюционный и сущностный аспекты. В: *Technical Science / «Colloquium-journal»*. 2019, №27 (51), с. 49-53. ISSN 2520-6990.

162. ШАНЬГИН, В.Ф. *Информационная безопасность компьютерных систем и сетей* Москва: ИД «ФОРУМ»: ИНФРА-М, 2012. 415 с. ISBN 978-5-8199-0331-5.

163. ШМИДТ, Э., КОЭН, Д. *Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств.* Москва: ООО «Манн, Иванов и Фербер», 2013. 368 с. ISBN 978-5-91657-824-9.

164. ШНАЙЕР, Б. *Практическая криптография, 2-е издание: протоколы, алгоритмы, исходные тексты на языке Си.* Москва: Триумф, 2002. 610 с.

165. ЯРОЧКИН, В.И. *Информационная безопасность*. 2-е изд. Москва: Академический проект; Гаудеамус. 2004. 544 с. ISBN 5-8291-0408-3.

166. ЯЩЕНКО, В. В. и др. *Введение в криптографию*. 4-е изд. Москва: МЦНМО, 2012. 348 с. ISBN 978-5-4439-0026-1.

Интернет источники

167. Europass: Digital competences – Self-assessment grid [online]. *Онлайн инструмент ЕС унифицированного сравнения квалификаций* , 2021 [citat 01.07.2021]. Доступен: europass.cedefop.europa.eu/sites/default/files/dc-en.pdf]

168. National Cyber Strategy of the United States of America [online]. *Сайт Архива Белого Дома при президенте Д. Трампе,* 2019 [citat 01.05.2019]. Доступен: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

169. Plan de învăţământ. Ştiinţe economice. [online]. *Сайт Institutul de Relații Internaționale din Moldova,2*021 [citat 01.02.2021]. Доступен: http://irim.md/wp-content/uploads/2016/05/Plan-de-invatamint-Economie-Mondiala-si-Relatii-Economice-Internationale-Ciclul-I.pdf

170. Plan de învăţământ. Ştiinţe economice. [online]. *Сайт Universitatea de Stat din Moldova,* 2021 [citat 01.02.2021]. Доступен: http://usm.md/wp-content/uploads/Marketing-si-logistica.pdf

171. Plan de învăţământ. Ştiinţe economice. [online]. *Сайт Academia de Studii Economice a Moldove,* 2021 [citat 01.02.2021]. Доступен: https://ase.md/files/planuri/2018/zi/EG.pdf

172. Plan de învăţământ. Ştiinţe [online]. *Сайт* Universitatea de Stat „Grigore Țamblac" din Taraclia, 2022 [citat 02.06.2020]. Доступен: https://tdu-tar.md/images/files/3_uchebnyy_process/5_knigi_specialjnsotey/Manualul_specialit_Uch.pdf

173. Plan de învăţământ. Ştiinţe economice. [online]. *Сайт Universitatea de Studii Europene din Moldova,* 2021 [citat 01.02.2021]. Доступен: https://www.usem.md/uploads/files/Facultatea_Stiinte_Economice/Planuri_de_invatamint/Ciclul_I/2017/Planuri/0413_1%20Business%20și%20administrare.PDF

174. *Институт ЮНЕСКО по информационным технологиям в образовании*. ИИТО

ЮНЕСКО © 1997-2022 [citat 23.10.2021]. Доступен: https://iite.unesco.org/ru/

175. Конгресс США. *Congress USA* © 2022 [citat 23.09.2021]. Доступен: https://www.congress.gov/bill/115th-congress/house-bill/4943.

176. Кибербезопасность в программе DIGITAL Europe [online]. *Цифровая Европейская Программа,* 2021 [citat 23.10.2021]. Доступен: https://digital-strategy.ec.europa.eu/en/activities/cybersecurity-digital-programme

177. Описание курса «Информационная безопасность». Сайт Департамента компьютерных наук Принстонского университета США, 2022. [citat 23.12.2021]. Доступен: https://www.cs.princeton.edu/courses/archive/fall21/cos432/

178. Отчет «Обеспечение навыков для новой экономики» [online]. *Сайт Конфедерации британской промышленности (CBI),* 2019 [citat 23.10.2021]. Доступен: www.cbi.org.uk/articles/delivering-skills-for-the-new-economy/

179. Отчет Ecorys «Digital skills for the UK economy 2016» [online]. *Информационный веб-сайт государственного сектора Соединенного Королевства*, 2016 [citat 23.10.2021]. Доступен: www.gov.uk/government/publications/digital-skills-for-the-uk-economy

180. Отчет OECD «Skills for a Digital World 2016» [online]. *Сайт Международного союза электросвязи (ITU),* 2016 [citat 23.10.2021]. Доступен: https://www.itu.int/en/ITU-D/Digital-Inclusion/Women-and-Girls/Girls-in-ICT-Portal/Documents/OECD%20skills%20for%20a%20digital%20world.pdf

181. Отчет ВЭФ «Principles for Board Governance of Cyber Risk» [online]. *Сайт Всемирного Экономического Форума (ВЭФ),* 2021 [citat 07.07.2021]. Доступен: http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf

182. *Официальный сайт РОЦИТ*. ИИТО ЮНЕСКО © 1996-2022 [citat 01.02.2021]. Доступен: цифроваяграмотность.рф

183. *Официальный сайт Технологического института SANS*. SANS Technology Institute, © 2022 [citat 23.12.2021]. Доступен: https://www.sans.edu

184. *Портал о программах бакалаврита по всему миру.* Keystone [citat 23.12.2021]. Доступен: https://www.bachelorstudies.co.uk/BSc/Cyber-Security/

185. *Портал Федеральных государственных образовательных стандартов высшего образования*, НИТУ «МИСиС». ©2021 [citat 28.12.2021]. Disponibil: http://fgosvo.ru/fgosvo/92/91/4/88 /

186. Семинар «Интеллектуальный анализ и прогнозирование экономической и финансовой преступности в кибернетической взаимосвязи деловой среды (fincrime)» [online]. *Сайт Университета Бабеша-Бойяи (UBB),* 2022 [citat 04.01.2021]. Доступен: https://news.ubbcluj.ro/event/workshopul-analiza-inteligenta-si-predictia-criminalitatii-

economice-si-financiare-intr-un-mediu-de-afaceri-interconectat-cibernetic-fincrime-desfasurat-la-ubb/

187. Учебный план для бакалавров информационных технологий 2016 год. Сайт Monash University in Melbourne Australia. 2022 [citat 23.12.2020]. Доступен: https://www.monash.edu/business

188. *Школа информационных технологий: Учебные планы*. TalTech, ©2022 [citat 04.01.2022]. Доступен: https://taltech.ee/en/bachelors-studies-it

189. Элективный курс «Информационная и экономическая безопасность» [online]. *Сайт Национальный исследовательский университет «Высшая школа экономики»,* 2022 [citat 12.01.2022]. Доступен: https://electives.hse.ru/minor_security_perm/

190. *Факультет экономики и делового администрирования: Учебные планы*. Universitatea Alexandru Ioan Cuza din Iași, ©2022 [citat 04.01.2022]. Доступен: https://www.feaa.uaic.ro/programe-de-licenta/planuri-de-invatamant/

Приложение 1. Выписки из официальных документов РМ

Из Постановления Парламента Республики Молдова об утверждении Стратегии информационной безопасности Республики Молдова на 2019–2024 годы и Плана действий по ее реализации следует, что решение задачи «1) «*развитие системы подготовки кадров в области информационной безопасности*» будет выполнено путем (статья 99):

«*1)* ***оценки текущего уровня подготовки кадров в области информационной безопасности по каждому разделу в отдельности: средства массовой информации, информационные технологии, оборона, общественный порядок и контрразведка****;*

2) установления категориями бенефициаров, подлежащих включению в приоритетном порядке в новые программы обучения кадров в указанной области;

3) разработки новых программ по подготовке кадров в области информационной безопасности;

4) разработки и внедрения учебных программ для работников с полномочиями по расследованию и уголовному преследованию, прокуроров, судей, специалистов и судебных экспертов в данной области в правоприменительных структурах, а также для технического персонала публичных учреждений».

Решение задачи ««*развитие культуры информационной безопасности*» будет выполнено путем (статья 88):

«*1) проведение действий по привлечению внимания и информированию общества относительно угроз, уязвимостей и рисков кибербезопасности;*

2) проведение Национальным центром реагирования на инциденты кибербезопасности стратегического анализа инцидентов кибербезопасности и согласование ответных действий на такие инциденты, в том числе посредством проведения специальных курсов квалифицированными экспертами;

3) проведение общих учений и тренировок по укреплению потенциала реагирования на кибератаки, в том числе по блокировке учебных кибератак;

4) организация и проведение тренингов в области кибербезопасности для персонала публичного и частного секторов, владельцев элементов критической инфраструктуры;

5) сертификация специалистов в области кибербезопасности специализированными организациями/компаниями, исходя из применяемых стандартов и утвержденных минимальных обязательных требований кибербезопасности;

6) организация кампаний по привлечению внимания и информированию относительно угроз в киберпространстве и мер защиты, которые могут быть приняты физическими и юридическими лицами;

7) ***введение и продвижение куррикулумного содержания об информационной безопасности в национальных учебных программах****;*

8) организация, в том числе совместно с иностранными партнерами, тематических учебных курсов в области кибербезопасности для работников публичных учреждений».

Приложение 2. Обзор определений понятия «информационная безопасность»

Арсеньтьев М. В.	Информационная безопасность – это снятие информационной неопределенности относительно объективно и субъективно существующих потенциальных и реальных угроз за счет контроля над мировым информационным пространством и наличия возможностей, условий и средств для отражения этих угроз, что в совокупности определяет уровень (степень) информационной безопасности каждого субъекта.	Арсентьев М.В. К вопросу о понятии «информационная безопасность». В: *Информационное общество*. 1997, № 4-6, с.48-50
Блинов А. М.	информационная безопасность – состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие	Блинов А. М. Информационная безопасность: Учебное пособие. Часть 1. Санкт-Петербург: Изд-во СПбГУЭФ, 2010. 96 с. С.17
Бондарев В. В.	Информационная безопасность – защищенность общества и личности от деструктивного информационного воздействия (пропаганды, агрессивной рекламы, низкопробных видов искусства и т. п.),	Бондарев, В. В. Введение в информационную безопасность автоматизированных систем: учебное пособие. Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. 250 с. С.16
Зима В.М Молдовян А.А.	Говорят о системном подходе: Под защитой информационно-программного обеспечения понимается использование средств и методов, принятие мер и осуществление мероприятий с целью обеспечения безопасности хранимой и обрабатываемой информации, а также используемых в ВС программных средств.	В. М. Зима, А. А. Молдовян Многоуровневая защита информационно-программного обеспечения вычислительных систем.– Санкт-Петербург: Ротапринт МГП "Поликом", 1997. 105 с. –С. 14
Вострецова Е. В.	Информационная безопасность — состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам)	Вострецова Е. В. Основы информационной безопасности : учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.– С.15
Герасименко В. А., Малюк	проблема информационной безопасности состоит в том, что, «современные технические, технологические и организационные системы, а также люди, коллективы людей и общество в целом сильно подвержены внешним информационным воздействиям, причем последствия негативного воздействия могут носить не просто тяжелый, а трагический и даже катастрофический характер.» Появилась «не только проблема защиты информации, но и защиты от информации»	Герасименко В.А., Малюк А.А. Москва: МИФИ, 1997. 537 с. С.50-51 ISBN: 5-88852-010-1
Емельянова Н. З.,	Информационная безопасность — состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.	Емельянова Н. З., Партыка Т. Л., Попов И. И. Защита информации в персональном компьютере учебное пособие. М.: ФОРУМ, 2009. 368 с. С. 348
Корнеев И. К., Степанов Е. А.	Информационная безопасность – составная часть экономической безопасности, направленная на разработку и актуализацию программы построения аналитической работы по определению состава ценной информации предприятия, угроз информации, по формированию системы защиты информации в	Корнеев И. К., Степанов Е. А. Защита информации в офисе : учеб. – М. : ТК Велби, Изд-во Проспект, 2008. – 336 с.

	традиционном и электронном документооборотах, защиты информации от персонала, защиты информации в технических каналах распространения информации и т. д.	
Курило А. П. член-корреспондент международной Академии информатизации, кандидат технических наук, доцент, заместитель начальника главного управления информационной безопасности и защиты информации Банка России,	ИБ – состояние защищенности информации, которое достигается обеспечением совокупности для нее свойств доступности, целостности, конфиденциальности, аутентичности, подотчетности, неотказуемости и надежности	Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. учебное пособие для вузов. — 2-е изд., испр. М.: Горячая линия-Телеком, 2014. 244 с. ISBN 978-5-9912-0361-6.
Мельников В. В.	Информационная безопасность РФ – состояние защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. (из Доктрины РФ)	Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для студ. высш.учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков.– 3-е изд.. М.: Издательский центр «Академия», 2008. 336 с
Нестеров С. А.	Безопасность информации — это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность (стр. 13)	Нестеров, С. А. Информационная безопасность: учебник и практикум для СПО М.: Издательство Юрайт, 2018. — 321 с. (Серия : Профессио нальное образование). ISBN 978-5-534-07979-1
Платонов В.В.	ИБ – защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.	Платонов В. В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования.– М.: Издательский центр «Академия», 2013.– 336 с. – С.13
Полякова Т. А., Стрельцов А. А.	ИБ – с одной стороны, состояние защищенности человека, общества и государства в информационной сфере, а с другой —результат деятельности по обеспечению информационной безопасности. В свою очередь, обеспечение информационной безопасности логично рассматривать как деятельность по противодействию угрозам безопасности человека, общества и государства в информационной сфере, осуществляемую с использованием выделенных для этого сил и средств.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. М. : Издательство Юрайт, 2016. 325 с.
Романец Ю. В.	Безопасность АСОИ защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, изменения или разрушения ее компонентов	Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина.– 2-е изд., перераб. и доп.– М.: Радио и связь, 2001.–376 с.– С.14
Стрельцов А. А. и	ИБ человека заключается в защищенности его	Стрельцов А. А., Пожарский, В. А.,

др.	интересов, связанных с информацией и информационной инфраструктурой, защищенностью его качеств как субъекта, использующего информацию для адаптации к изменениям окружающей, в том числе социальнйо действительности, от угроз ущемления его интересов, от нанесения вреда его личности, деятельность котрой во многом базируется на осмыслении получаемой информации, информационных воздейтсвий с другими индивидами и часто использует информацию в качестве предмета деятельности (стр. 21) ИБ организации – защищенность от угроз ущемления ее интересов, связанных сполучением, обработкой, хранением, передачей, распространением информации, от угроз нарушения установленных режимов функционирования информационных систем и использования телекоммуникационных ресурсов, а также от угроз нарушения конфиденциальности определенной информации, которую оранизация хотела бы сохранить в неизвестности для других лиц (стр. 22-23) Иб государства – защищенность от угроз его способности получать, обрабатывать, хранить, передавать и распространять информацию, необходимую для управления обществом, выполнения законодательной, правоприменительной и судебной функций, а также сохранять определенную часть информации в тайне от других лиц (стр. 24-25)	Минаев, В.А., Тарапанова Е. А., Фролов Д. Б., Скрыль С. В., Сычев А. М., Коробец, Б. Н., Вайц, Е. В., Грачева, Ю. В., Астрахов, А. В. Организационно-правовое обеспечение информационной безопасности. Под. ред. Александрова А. А., Сычева М. П. Москва: Издательство МГТУ им. Н. Э. Баумана, 2018. 291 с. ISBN 978-5-7038-4723-7/
Урсул А. Д.	информационная безопасность - это способность государства, общества, социальной группы, личности, во-первых, обеспечить с определенной вероятностью достаточные и защищенные социальный интеллект и информационный ресурс, оптимальную социальную энтропию и инфосреду для поддержания жизнедеятельности и жизнеспособности, устойчивого функционирования и развития социума; во-вторых, противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации; в-третьих, вырабатывать личностные и групповые навыки и умения безопасного поведения; в-четвертых, поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано; в-пятых, постоянно и последовательно по определенной безопасной программе "вмонтировать" искусственный интеллект в социосреду. В такой интерпретации информационная безопасность проявляется не только как один из видов безопасности, но и как срез тех ее видов в сфере действия которых индустрия информатики занимают важное место.	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. СУЩНОСТЬ, СОДЕРЖАНИЕ И ПРИНЦИПЫ ЕЕ ОБЕСПЕЧЕНИЯ А.Д.Урсул Т. (Ф.) Н, [online] disponibil https://security.ase.md/publ/ru/pubru22.html

Шаньгин В. Ф.	Информационная безопасность – защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар) и т. п.	Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2011. 416 с.– С.11
Ясенев В.Н	Информационная безопасность – невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз).	Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: Учебное пособие. Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. 198 с.– С.8

Приложение 3. Современные определения информационных угроз

Триада угроз CIA: 1975 и современное определение

Угрозы ИБ		Определение	
		Джеймс Андерсон, Джерри Зальцер, Майкл Шрёдер (1975)	Современные стандарты в области ИБ
C	конфиденциальность (confidentiality),	неавторизованное раскрытие информации (англ. unauthorized information release): неавторизованное лицо может получить и использовать компьютерную информацию, либо провести несанкционированный анализ трафика, либо незаконно воспользоваться коммерческой программой	угроза нарушения конфиденциальности: несанкционированное разглашение информации
I	целостность (integrity)	неавторизованное изменение информации (англ. unauthorized information modification): неавторизованное лицо в форме саботажа может вносить изменения в хранящуюся информацию, не обязательно известную злоумышленнику	угроза нарушения целостности: несанкционированное изменение или удаление информации
A	доступность (availability)	неавторизованный отказ в доступе (англ. Unauthorized denial of use) к информации: злоумышленник, также в форме саботажа, может организовать сбой в системе, модифицировать алгоритм или повредить компьютерную технику с тем, чтобы помешать авторизованному пользователю прочитать или изменить информацию, при этом злоумышленник может и не иметь возможности ссылаться на информацию или изменять ее	угроза нарушения доступности: несанкционированный запрет авторизированному пользователю к информации в момент необходимости

Приложение 4. Краткая характеристика он-лайн ресурсов

Joomag — многофункциональная платформа цифрового издательства для создания интерактивного контента, многоканального распространения, отслеживания результатов. Может использоваться для создавания и публикации электронных книг образовательной направленности. Joomag в базовой бесплатной версии содержит сотни шаблонов, которые можно использовать для создания весьма содержательной электронной книги, которую можно сохранить отдельной ссылкой в своём аккаунте, встроить в сайт или блог.

Testmoz – он-лайн конструктор тестов. Его используют, начиная с 2008 года, более 1 млн. пользователей по всему миру. Сервис не требует регистрации и оплаты. Существует платная версия с дополнительными функциями.

После создания теста разработчик получает уникальную ссылку, по которой можно пройти тест. При желании можно создать пароль, чтобы тест был доступен только тем, кому предназначены задания. По этой же ссылке разработчик может зайти как администратор, указав свой пароль. Администратор тестов на вкладке «Отчеты» видит, кто, когда решал тест и на сколько вопросов ответил правильно. После окончания теста испытуемый может ознакомиться с результатом и увидеть свои ошибки.

Данная система очень удобна в использовании, имеет простой и интуитивно понятный интерфейс. Сервис поддерживает вопросы типов:

– выбор одного правильного варианта из многих;

– выбор несколько правильных варианта из многих;

– альтернативный вопрос (истина или ложь);

– открытый вопрос (студент вписывает ответ в пустое поле).

Баллы рассчитываются автоматически в зависимости от веса каждого правильного ответа. Сервис комбинирует расположение вопросов внутри теста и ответов внутри вопроса, что позволяет создавать множество вариантов тестовых заданий. Уровень освоения учебного материала определяется путем статистической обработки ответов:

– процент правильных ответов по каждому вопросу;

– процент правильных ответов у каждого студента.

GoogleSites – GoogleSites – бесплатный конструктор и хостинг. Для работы с ним не требу¬ется знание веб-программирования. Его можно использовать для совместного редактирования. Разработчику предоставляется множество инструментов. Сервис предоставляет 100 МБ свободного пространства. Этого достаточно для создания учебного сайта.

Приложение 5. Тематический веб-квест: «Информационная безопасность для экономистов»

Тематический веб-квест:
«Информационная безопасность для экономистов»

Исполнитель: Богданова Виолетта Алексеевна,
преподаватель кафедры «Информационные и электроэнергетические системы»
Бендерского политехнического филиала «ПГУ им. Т.Г. Шевченко»,
преподаватель высшей квалификационной категории
(информационные дисциплины)

Адрес: MD-3200, г. Бендеры, ул. Бендерского Восстания, 7, моб. +37377894573;
e-mail: bogdanovaleta@gmail.com

sites.google.com/view/bogdanova-zki/главная

Бендеры, 2019

ОПИСАНИЕ ОБРАЗОВАТЕЛЬНОГО ПОРТАЛА

Во всемирной паутине имеются многообразные ресурсы, содержащие материал, потенциально учебного характера. Проблема состоит в том, что информация, которую находят обучающиеся, не всегда актуальна, адекватна и безопасна. Решить эту проблему можно с помощью технологии веб-квест. В рамках данной информационно-коммуникационной педагогической технологий педагог может формировать поисковую, познавательную деятельность учащихся в сети Интернет с учетом актуальности, адекватности и безопасности [1]. Данная технология относится к игровым методам обучения.

Обучающиеся выбирают заранее предложенные преподавателем роли и работают каждый в своем направлении. В итоге каждый обучающийся получает весь объем информации, но по своему индивидуальному «маршруту знаний». Преподаватель ставит конкретные задачи на каждом этапе и определяет сроки выполнения. Обучающиеся переходят к следующему этапу, успешно выполнив задания предыдущего. Работа в рамках веб-квеста состоит в получении информации во всемирной паутине под руководством преподавателя.

Тематический квест по теме «Информационная безопасность для экономистов» предназначен для студентов, обучающихся по направлению подготовки бакалавра 38.03.01 «Экономика», при изучении дисциплины Б1.В.ДВ.5.1. «Информационная безопасность». Также данный квест целесообразно использовать в самостоятельной работе студентов при изучении дисциплин информационного цикла, т.к. Федеральный государственный образовательный стандарт высшего образования РФ уровень высшего образования бакалавриат направление подготовки 38.03.01 Экономика от 12.11.2015 предписывает: «Выпускник, освоивший программу бакалавриата по направление подготовки 38.03.01 Экономика должен обладать следующими общепрофессиональными компетенциями: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований *информационной безопасности* (ОПК-1)» [2].

В результате прохождения веб-квеста, студенты должны усвоить:

– нормативно-правовые аспекты информационной безопасности;

– морально-этические нормы аспекты информационной безопасности;

– организационные средства средства защиты информации;

– технические, программные и физические средства защиты информации.

Предлагаемый квест размещается по адресу **sites.google.com/view/bogdanova-zki/главная.** Тематический квест по информационной безопасности содержит разделы (вкладки): главная, роли, сроки, тест.

Вкладка Главная. На вкладке Главная расположен видеоролик об одной из актуальных угроз человечеству – информационной безопасности. Также там расположена ссылка на методические указания, разработанные автором, средствами цифровой платформы Joomag. Данные задания помогают сформировать практические навыки защиты информации.

Для участия в веб-квест студентам необходимо распределиться на три группы, каждая из которых изучает и готовит материалы с точки зрения информационной безопасности:

I – дома,

II– офиса,

III – государства.

Вкладка Роли. Каждый студент выбирает себе роль, которая предполагает выполнение фиксированных заданий. Для качественного выполнения заданий необходимо перейти по ссылке соответствующей роли, где педагогом подобраны информационные

ресурсы с учетом актуальности, адекватности и безопасности [3].

Квест предусматривает такие роли для студентов как правовед, психолог, практик, администратор, аналитик и ошибковед. Правовед более глубоко изучает законодательные аспекты работы с информацией, определяет что и как защищать с точки зрения норм юридического права. Психолог подробно рассматривает морально-этические нормы использования информации. Практик углубляется в программные средства защиты информации, администратор – в технические. Аналитик изучает организационные средства защиты информации, в частности международные и российские стандарты в области информационной безопасности. Ошибковед занимается поиском типичных уязвимостей в системе защиты информации.

Каждый участник квеста формирует отчет (в форме компьютерной презентации, схемы, таблицы, памятки и т.п), на базе которого предусматривается составление итогового отчёта группы. Перечень материалов, которые готовят участники, в зависимости от роли и с учетом специализации команды (информационная безопасность дома, офиса или государства).

Правовед готовит:

- перечень законодательных и нормативных актов в области информационной безопасности;
- опорный конспект темы «Законодательные средства защиты информации»;
- структурную схему системы понятий типов информации в зависимости от доступа.

Психолог готовит**:**

- памятку по этическим нормам применения информационных технологий;
- памятку защиты от воздействия социального инженера.
- сравнительный анализ этических норм разных стран.

Практик готовит:

- карту свободно распространяемых программных средств в области защиты информации;
- подборку свободно распространяемых антивирусов.

Администратор готовит**:**

- презентацию «10 способов технического перехвата информации»;
- памятку «10 золотых правил технической защиты информации».

Аналитик готовит**:**

- хронологию создания стандартов в области информационной безопасности;
- перечень важнейших международных стандартов в области информационной безопасности с указанием сферы их применения.

Ошибковед готовит**:**

- банк типичных ошибок в области защиты информации;
- памятку «Так нельзя работать с информацией».

Вкладка Сроки. В данном разделе студенты могут ознакомиться с крайними сроками выполнения задания. По завершению квеста, группы выступают с защитой отчетов и обучаемые совместно с педагогом взаимно оценивают проделанную работу.

Вкладка Тест. Все участники в индивидуальном порядке проходят тест, после окнчания веб-квеста. Пароль необходимо получить у преподавателя. Сделано это для того, чтобы можно было проанализировать, кто решал тест и на сколько вопросов ответил правильно, с какими вопросами справились все участники, а какие вызвали наибольшие затруднения.

Отличительной особенностью предложенного веб-квеста является сам инструмент GoogleSites. Применение веб-квест технологии в обучении требует некоторых информационных компетенций со стороны преподавателя. GoogleSites – бесплатный конструктор и хостинг. Для работы с ним не требуется знание веб-программирования. Его можно использовать для совместного редактирования. Разработчику предоставляется

множество инструментов (рис.).

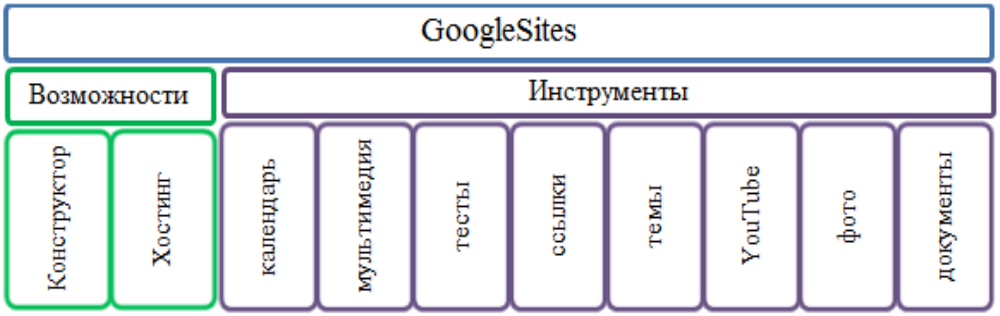


Рисунок . Инструменты и возможности GoogleSites

Сервис предоставляет 100 МБ свободного пространства. Этого достаточно для создания учебного сайта. Ссылки на проверенные интернет ресурсы, видеоролики, мультимедия и другие элементы позволяют создать дружественный интерфейс.

Разработанный сайт можно адаптировать для мобильных устройств. Студенты часто используют именно их в учебной деятельности. Google Forms позволяет создать анкеты, тесты. Сервис предоставляет возможность анализа данных с помощью инструмента Google Analitics. Результаты можно просматривать в виде сводки, CSV-файла, а также в отдельной таблице. В разрабатываемый сайт можно интегрировать Google документы, таблицы и презентации.

ИНСТРУКЦИЯ ДЛЯ ПРЕПОДАВАТЕЛЯ

1. Прежде чем предложить квест студентам, выполните его сами.
2. Перед началом работы с квестом проведите инструктаж с учащимися. Продемонстрируйте примеры выполнения подобных квестов. Укажите на наиболее типичные ошибки.
3. Укажите временные рамки.
4. Предложите студентам выбрать 3 капитанов. Объясните капитанам, что они несут ответственность за успех команды.
5. Предложите выбранным капитанам по жребию набрать себе команду.
6. Предложите студентам выбрать себе роли.
7. По завершению квеста, группы студентов выступают с защитой отчетов и обучаемые совместно с педагогом взаимно оценивают проделанную работу.
8. Проведите оценивание работ с точки зрения полноты исполнения заданий. Предложите студентам участвовать в оценке результатов работы.
9. Определите победителей.
10. Дайте пароль студентам и проведите тестирование.
11. По аналогии с представленным квестом, Вы можете разработать свои квесты для различных тем и разделов.

ИНСТРУКЦИЯ ДЛЯ СТУДЕНТОВ

1. Следует внимательно ознакомиться с главным заданием и предлагаемыми ролями квеста. Только после этого выбрать себе роль.
2. Необходимо вдумчиво и последовательно выполнять задания своей роли.
3. При выполнении заданий важно использовать ресурсы, указанные преподавателем в разделе «Роли». Дополнительные источники приветствуются при условии, что они будут носить вспомогательный характер.
4. Следует помнить, что время выполнения квеста ограничено (преподавателем).
5. Для прохождения теста получите у преподавателя пароль. Проанализируйте правильность своих ответов. Обсудите их с преподавателем и другими участниками квеста.
6. Помните, что не ошибается тот, кто ничего не делает!

Желаю успеха!

Сайт для веб-квеста «Информационная безопасность» реализован средствами Google Sites

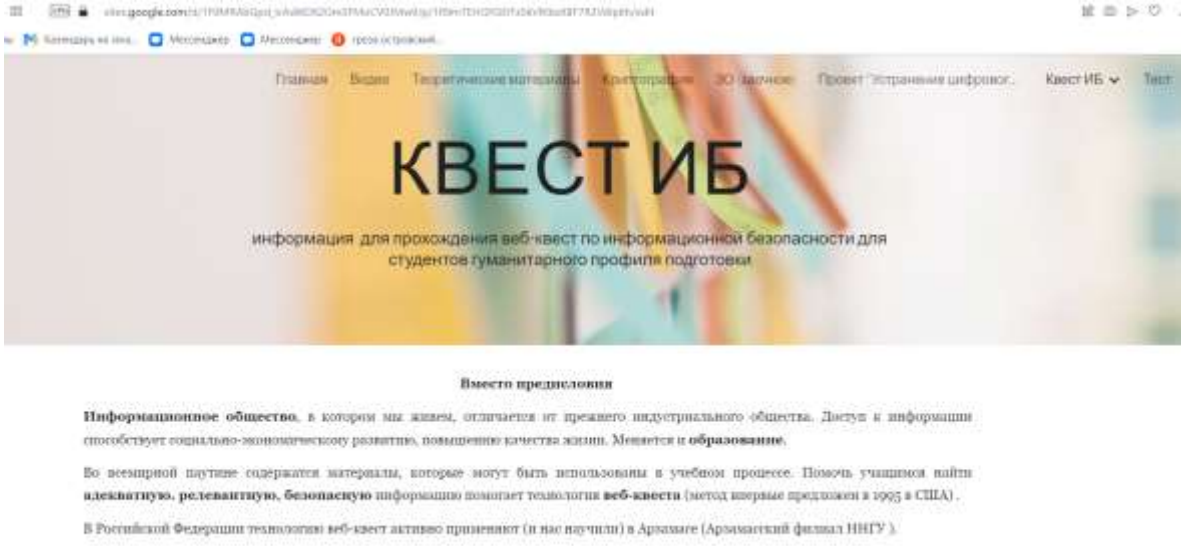


Рис. 5.1. Вкладка «Квест ИБ»

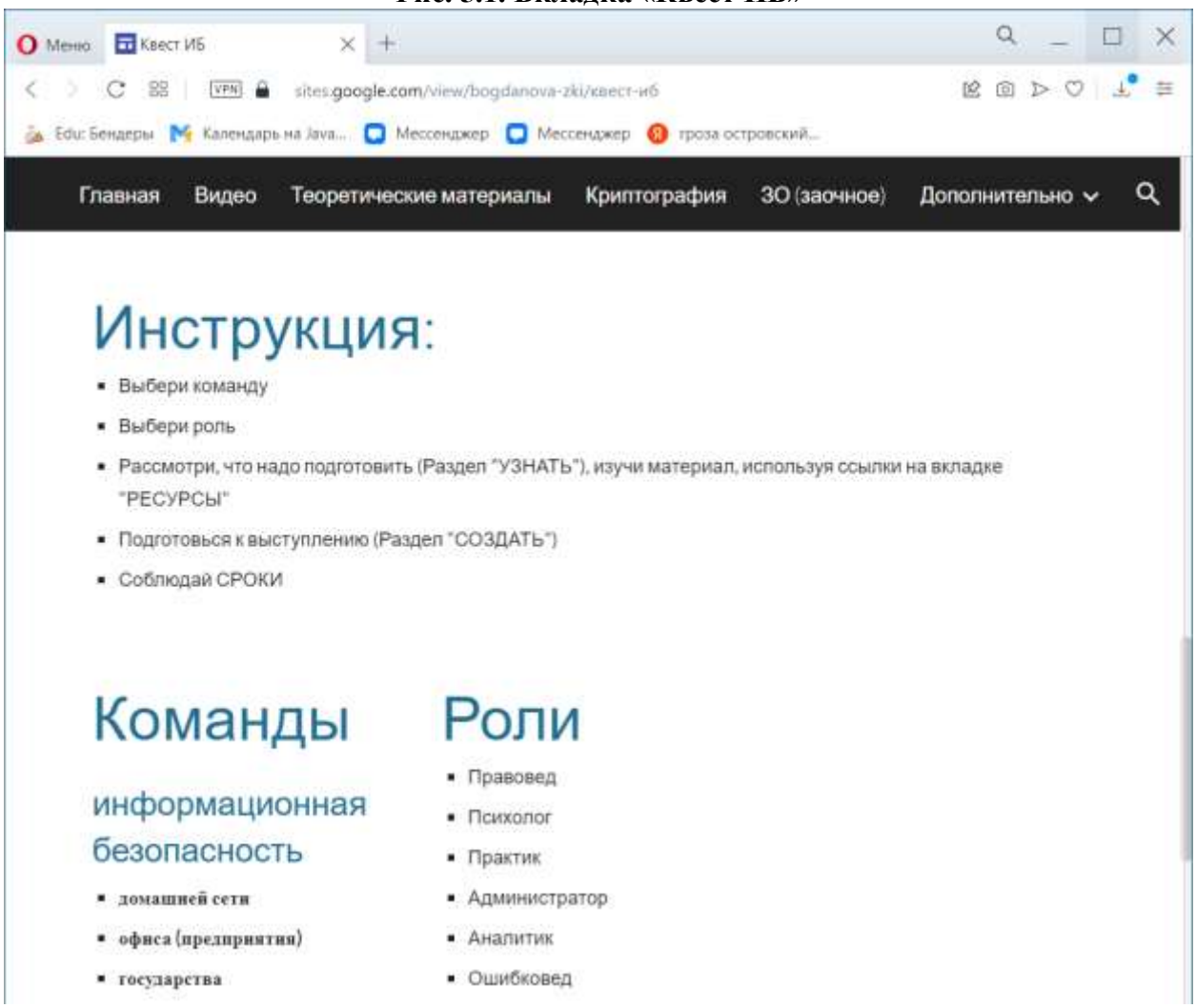


Рис. 5.2. Вкладка «Инструкция»

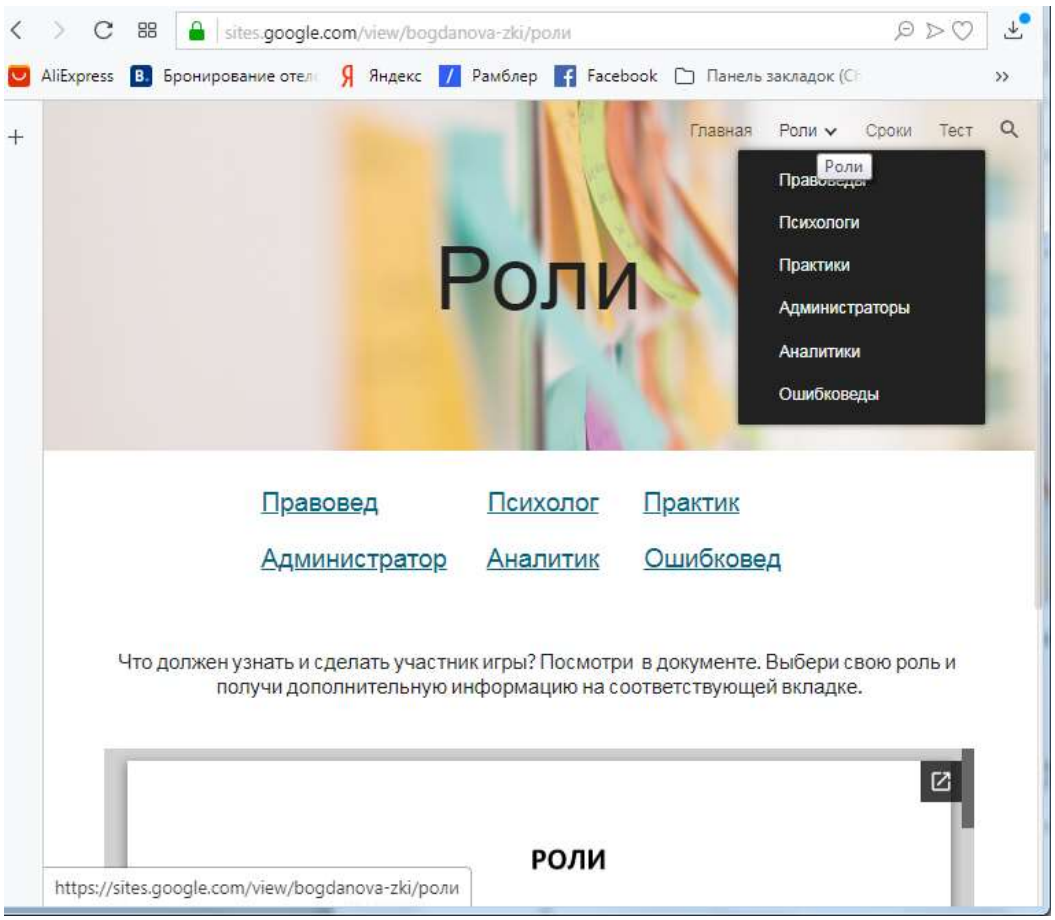


Рис. 5.3. Вкладка «Роли»

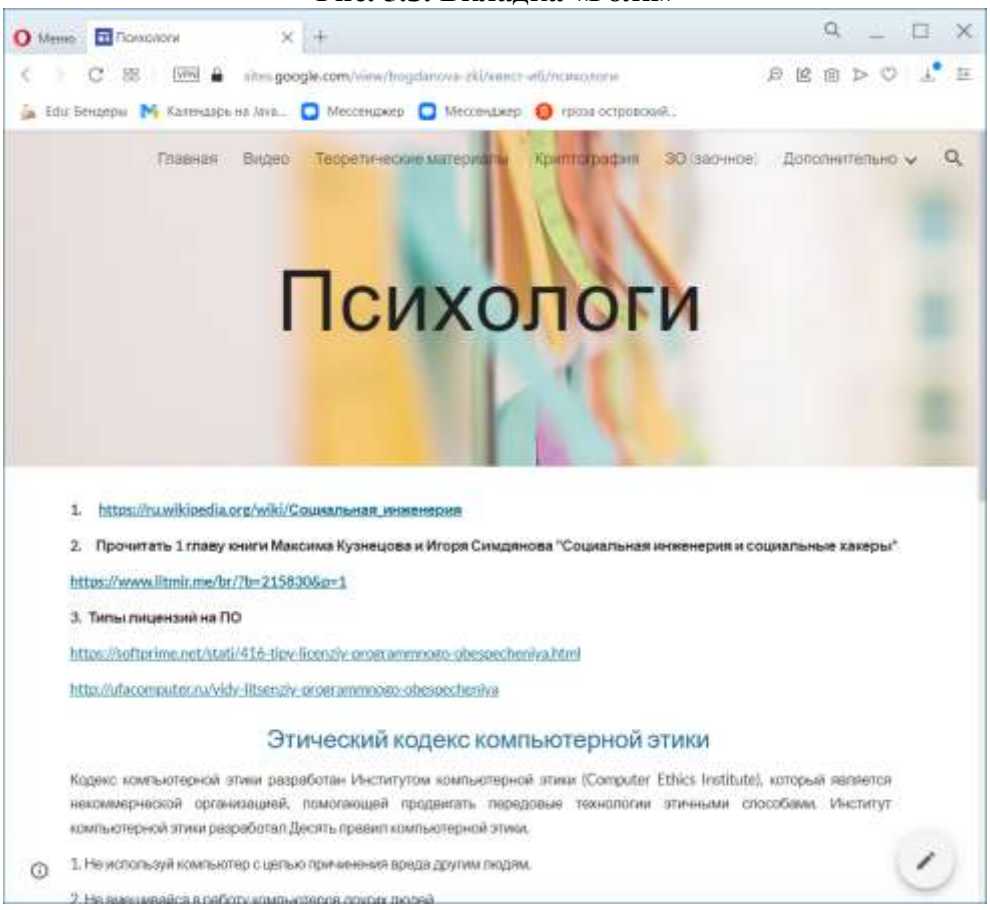


Рис. 5.4. Вкладка «Роль Психолог»

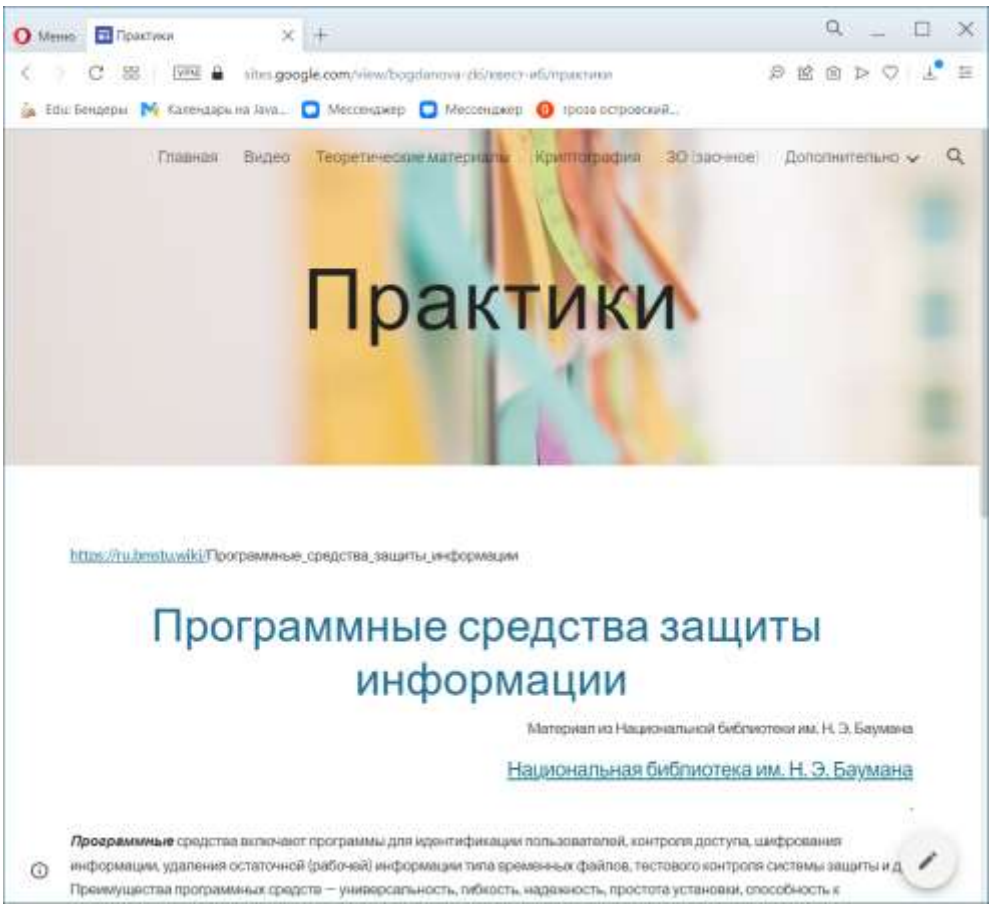


Рис. 5.5. Вкладка «Роль Практик»

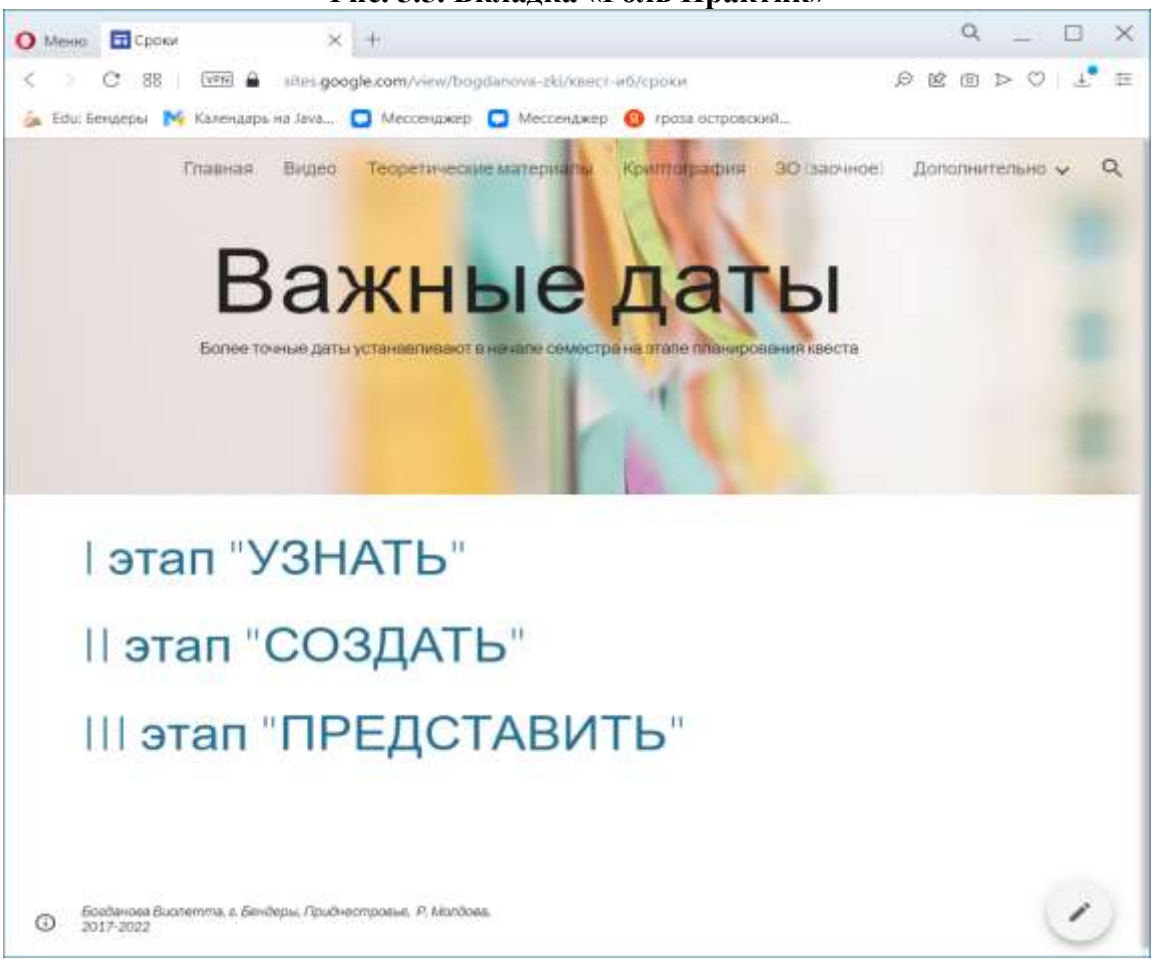


Рис. 5.6. Вкладка «Важные даты»

Приложение 6. Итоговый тест по дисциплине «Информационная безопасность»

Инструкция к тесту

На выполнение тестовых заданий предусмотрено 60 минут. Задания разделены на 4 уровня сложности и содержат вопросы по 6 разделам курса. Для организации тестирования используется он-лайн конструктор тестов TestMoz.com.

Представлены 4 типа тестовых заданий:

– множественный выбор (может быть несколько правильных вариантов ответа на вопрос, обозначается кнопкой типа CheckBox – флажок включен ☑, выключен ☐);

– одиночный ответ – выбор одного правильного варианта из нескольких, обозначается кнопкой типа RadioButton – переключатель○;

– альтернативный вопрос – определение истинно или ложно утверждение;

– вопрос со свободным ответом – пользователь должен написать слово, в каждом вопросе такого типа указано количество букв, содержащихся в правильном ответе.

Раздел 1. Основные понятия и угрозы ИБ

I уровень

1. В современном мире информация становится

A. Стратегическим ресурсом государства +
B. Товаром +
C. Бумажной документацией
D. Производительной силой +

2. К основным составляющим информационной безопасности относятся

A. Конфиденциальность +
B. Целостность +
C. Доступность +
D. Надежность

II уровень

1**. Под угрозой безопасности информации понимается**:

A. Атака на информацию со стороны злоумышленника
B. Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации +
C. Несанкционированный доступ к информации, который может привести к нарушению целостности системы компьютерной безопасности

2. К каналам утечки информации относятся:

A. Электромагнитный +
B. Аудио-визуальный +
C. Интернет и Wi-Fi
D. Социальный +

III уровень

1. Основные виды случайных угроз:

A. Стихийные бедствия и аварии, а также сбои и отказы технических средств +
B. Ошибки при разработке компьютерных систем, алгоритмические и программные ошибки +
C. Ошибки пользователей и обслуживающего персонала +
D. Электромагнитные излучения, наводки, а также вредительские программы

2. Основные виды преднамеренных угроз:

A. Алгоритмические и программные ошибки
B. Шпионаж и диверсии, несанкционированный доступ (НСД) к информации +
C. Электромагнитные излучения и наводки +
D. Стихийные бедствия и аварии, а также сбои и отказы технических средств
E. Вредительские программы +

IV уровень

1. **Известность содержания информации только имеющим соответствующие полномочия субъектам** – это_____ (18 букв)

(Конфиденциальность)

2. Основные направления по защите информационной собственности

A. Государственная тайна+
B. Коммерческая тайна +
C. Персональные данные +
D. Интеллектуальная собственность +
E. Банковская тайна +
F. Служебная тайна +

1. Верно ли утверждение: Стоимость защиты не должна превышать стоимость самой информации

A. Правда
B. Ложь +

Раздел 2. Законодательные средства ИБ

I уровень

1. Засекречиванию подлежат сведения о…

A. состоянии демографии
B. состоянии преступности
C. фактах нарушения прав и свобод человека и гражданина
D. силах и средствах обороны +

II уровень

1. Информационная безопасность личности включает в себя:

A. жизненно важные интересы личности и возможные угрозы им
B. защиту государственной информационной системы и информационных ресурсов
C. условия и факторы, создающие опасность жизненным интересам личности, общества и государства
D. соблюдение и реализацию конституционных прав на поиск, получение прав и распространение информации+

III уровень

1. Доступность информации заключается в том, что:

A. Любое лицо может получить доступ к информации.
B. Обладатель информации не установил никаких ограничений на доступ к ней.
C. Не существует препятствий для доступа к информации лица, которому обладатель информации предоставил доступ.+
Д. Информация подверглась распространению

IV уровень

1. Режим защиты информации не устанавливается в отношении сведений, относящихся к …

A. Государственной тайне
B. Деятельности государственных деятелей +
C. Конфиденциальной информации
D. Персональным данным

Раздел III. Средства защиты компьютерной информации

I уровень

1. Отметьте формальные средства защиты информации

A. Физические +
B. Законодательные
C. Программные +
D. Аппаратные +
E. Морально-этические
F. Организационные

II уровень

1.**Управление доступом – это**:

A. Идентификация пользователей, персонала и ресурсов системы (присвоение персонального имени, кода, пароля и опознание по предъявленному идентификатору) +
B. Криптографическая обработка защищаемой информации
C. Проверка полномочий (соответствия дня недели, времени суток, а также запрашиваемых ресурсов и процедур установленному регламенту) +
D. Регистрация обращений к защищаемым ресурсам +

E. Реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий +

2. Разработка и реализация комплексов мероприятий, создающих такие условия, при которых возможности несанкционированного доступа к защищаемой информации сводились бы к минимуму

A. Управление доступом
C. Шифрование
B. Регламентация +
D. Препятствие

III уровень

1. К программным средствам защиты информации не относятся:

A. Брандмауэр, архиватор, программа очистки, антивирус
B. Текстовый редактор, электронная таблица, брандмауэр
C. Текстовый редактор, электронная таблица, антивирус
D. Текстовый редактор, электронная таблица, браузер +

2. К организационным средствам защиты относят?

A. Использование антивирусов
B. Допуск только проверенных лиц к конфиденциальной информации +
C. Контроль доступа к памяти компьютера
D. Ввод системы контрольных битов с целью идентификации

IV уровень

1. При организации парольной защиты необходимо выполнять следующие рекомендации

A. Пароль не должен запоминаться субъектом доступа
B. Пароли должны периодически меняться +
C. В компьютерной системе должен храниться не сам пароль, а его хеш-значение +
D. Пароль должен выводиться на экран монитора
E. Пароль должен легко запоминаться и при этом быть сложным для отгадывания +

2. Запись пароля повышает вероятность его компрометации

A. Правда +
B. Ложь

Раздел 4. Идентификация и аутентификация. Пароли

I уровень

1. Какие средства аутентификации Вы знаете?

A. Биометрическая, статическая, парольная
B. Парольная, биометрическая, токен +
C. Динамическая, статическая, токен

II уровень

2. Не относятся к организационным мерам защиты

A. Проверка ПК на вирусы +
C. Разграничение прав доступа
B. Еженедельная смена пароля
D. Установка сигнализации +

III уровень

1. Какой уровень доступа считается наивысшим:

A. Чтение B. Редактирование C. Удаление + D. Добавление

IV уровень

1. Проверка подлинности – это _____(14 букв)

(Аутентификация, аутентификация, АУТЕНТИФИКАЦИЯ)

Раздел 5. Основы криптографии

I уровень

1. Шифр, использующий различные ключи для шифрования и дешифрования, называемые соответственно открытым и закрытым ключом называется:

A. Симметричный шифр
C. Гибридный шифр
B. Асимметричный шифр +
D. Шифр Гронсфельда

II уровень

1. Метод надежной передачи информации по открытому каналу связи использует:

A. Криптографию +
C. Кодирование
B. Стеганографию
D. Скремблирование

III уровень

1. Замену символов открытого текста соответствующими символами алфавита криптотекста называют:

A. простейшим шифром
C. шифром подстановки +
B. блочным шифром
D. ассимметричной замены

IV уровень

1. В чем состоят принципы Керкхоффса?

A. Алгоритм шифрования неизвестен, ключ неизвестен
B. Алгоритм шифрования известен, ключ неизвестен +
C. Систему шифрования необходимо сохранять в тайне
D. Система шифрования должна быть сложной +

Раздел 6. Электронно-цифровая подпись и алгоритм хеширования

I уровень

1. К свойствам ЭЦП относятся:

E. достоверность и неподдельность +
F. неотрицаемость +
G. невозможность использовать повторно +
H. невозможность изменить подписанный документ +

2. Цифровая подпись - …

A. подпись, которая ставится на документах
B. небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом, по которому можно удостоверится в аутентичности документа +
C. код с исправлением ошибок
D. имитоприставка

II уровень

1. Какая арифметика используется в алгоритмах ЭЦП?

A. Школьная
C. Компьютерная
B. Модульная +
D. Формальная

2. Функция, предназначенная для сжатия подписываемого документа до нескольких десятков, или сотен бит называется

A. логарифмической функция
C. хэш- функция +
B. сжимающая функцией
D. электронно-цифровая подпись

III уровень

1. Функции, для которых легко найти функцию прямого отображения и нельзя найти обратное называются:

A. линейные функции
C. односторонние функции +
B. нелинейные функции
D. функции преобразования

2. Широко известна *атака на основе парадокса* “_____” В математической статистике известен стандартный парадокс: «Должно собраться 23 человека, чтобы с вероятностью 1/2 хотя бы у двоих из них был общий день рождения».

A. математики
C. бумеранга
B. дней рождений +
D. информатики

IV уровень

1. Отметьте алгоритмы ЭЦП

A. ГОСТ Р34.10-94 + B. Эль Гамаля + C. DSA + D. RSA+

2. Правда ли, что открытый ключ позволяет вычислить секретный ключ?

А. Правда
Б. Ложь

Приложение 7. Анкета «Курс «Защита компьютерной информации» глазам студента»

АНКЕТА курс «Защита компьютерной информации» глазами студента
. Отношение к предмету а) положительное б) отрицательное в) равнодушное
2. Что понравилось в курсе «ЗКИ»: _____ _____
3. Укажите слабые стороны в курсе «ЗКИ»: _____ _____
4. Что бы хотелось узнать в области защиты информации: _____ _____
5. Материал излагался: а) доступно б) не доступно в) по-разному
6. Объективность в оценке знаний студентов: а) объективное б) необъективное
7. Просьба указать, какую часть занятий вы посетили (в %):
8. Необходима ли данная дисциплина в подготовке будущих экономистов? а) да б) нет в) не знаю
Подписывать анкету не нужно!

Рис. Анкета «Курс «Защита компьютерной информации» глазами студентов»

Приложение 8. Пример Рабочей программы дисциплины «Информационная безопасность»

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«Приднестровский государственный университет им. Т.Г. Шевченко»

Бендерский политехнический филиал

Кафедра «Инженерные науки, промышленность и транспорт»

УТВЕРЖДАЮ
И.о. директора БПФ ГОУ «ПГУ им. Т.Г. Шевченко»
Иванова С.С.
_____
(подпись, расшифровка подписи)
"____" _____20__ г

РАБОЧАЯ ПРОГРАММА

на 2021/2022 учебный год

для набора 2019 года

Учебной дисциплины

Б1.В.ДВ.03.01«*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Направление подготовки:
5.38.03.01 Экономика

Профиль подготовки
Экономика предприятий и организаций
(наименование профиля подготовки)

квалификация (степень) выпускника
Бакалавр

Форма обучения:
Очная

(в комбинированном формате)

Бендеры 2021

Приложение 9. Исходные данные уточняющего эксперимента

Таблица. Экранные формы экспериментальных данных в SPSS

2017-2018 осенний семестр

	FIO	Note	TypeGroup
1	Kus...	24	1
2	Uru...	43	1
3	Ko...	67	1
4	Cas...	45	1
5	Kar...	31	1
6	201...	39	1
7	Gafi...	43	1
8	201...	41	1
9	201...	25	1
10	ED-...	37	1
11	katia	69	1
12	Ulia K	65	1
13	Mari...	25	1
14	201...	63	1
15	ED-...	16	1
16	201...	35	1
17	201...	24	1
18	201...	18	1
19	Kob...	33	2
20	Doli...	24	2
21	Kud...	49	2
22	МД...	22	2
23	Ver...	37	2
24	Sail...	29	2
25	Ann...	16	2
26			

2017-2018 весенний семестр

	FIO	Note	Type(roup
1	2018_312_Ди...	37	2
2	2018_312_Ал...	53	2
3	2018_312_Go...	43	2
4	2018_312_Ди...	47	2
5	2018_312_Ко...	53	2
6	2018_312_Тю...	41	2
7	2018_312_Вр...	51	2
8	2018_312_Го...	69	2
9	2018_312_Ge...	51	2
10	2018_312_Ры...	24	2
11	2018_312_Ж ...	22	2
12	2018_312_No...	18	2
13	2018_312?_П...	43	2
14	2018_312_Ни...	55	2
15	2018_312_no...	59	2
16	2018_312_Ме...	24	2
17	2018_312_Ве...	39	2
18	2018_312_Sa...	25	2
19	2018_212_Tu...	39	1
20	2018_212_Gr...	45	1
21	2018_212_Ge...	63	1
22	2018_212_Ме...	45	1
23	2018_212_sh...	47	1
24	2018_212_Бо...	57	1
25	2018_212_An...	37	1
26	2018_212_Bu...	63	1
27	2018_212_Ty...	37	1
28	2018_212_Ка...	39	1
29	2018_212_Ya...	12	1
30	2018_212_Sp...	55	1
31	2018_212_Vl...	35	1

2018-2019 осенний семестр

	FIO	Note	TypeGroup
1	2018_Md-15Радо...	22	1
2	2018_МД-15 Жо...	24	1
3	2018_МД-15_Кю...	34	1
4	2018_МД-15_Ро...	34	1
5	2018_МД-15_Би...	39	1
6	2018_МД-15_Ор...	45	1
7	2018_МД-15_Су...	51	1
8	2018_МД-15_Ан...	57	1
9	2018_МД-15_Ан...	67	1
10	2018_ЭД-15_Ал...	22	2
11	2018_ЭД-15-Бе...	24	2
12	2018_ЭД-15_Во...	26	2
13	2018_ЭД-15_Ол...	32	2
14	2018_ЭД-15_Тк...	32	2
15	2018_ЭД-15_Го...	34	2
16	2018_ЭД-15_Ки...	34	2
17	2018_ЭД-15_Го...	35	2
18	2018_ЭД-15_Го...	37	2
19	2018_ЭД-15_Уз...	39	2
20	2018_ЭД-15_См...	41	2
21	2018_ЭД-15_Бе...	43	2
22	2018_ЭД_15_Ас...	45	2
23	2018_ЭД-15_Сл...	45	2
24	2018_ЭД-15_Яц...	47	2
25	2018_ЭД-15 Сай...	51	2
26	2018_ЭД-15_Ба...	51	2
27	2018_ЭД-15 Коч...	55	2
28	2018_ЭД-15_До...	55	2
29	2018_ЭД-1-15_Г...	65	2
30	2018_ЭД-15_Ка...	65	2
31	2018_ЭД-15_Ко...	71	2

Приложение 10. Описательная статистика уточняющего эксперимента

Количественное описание основных статистических показателей результатов итогового тестирования в рамках уточняющего эксперимента выполнено средствами SPSS

Таблица 10.1. Описательная статистика 2017-2018 осенний семестр в SPSS

Описательные статистики TypeGroup =EG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	18 18	16	69	39,44	16,978	288,261	0,540	0,536	-0,793	1,038

Описательные статистики TypeGroup = KG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	7 7	16	49	30,00	10,924	119,333	0,672	0,794	0,388	1,587

Таблица 10.2. Описательная статистика 2017-2018 весенний семестр в SPSS

Описательные статистики TypeGroup =EG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	13 13	12	63	**44,15**	13,771	189,641	-0,687	0,616	1,348	1,191

Описательные статистики TypeGroup = KG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	18 18	18	69	**41,89**	14,483	209,752	-0,138	0,536	-0,813	1,038

Таблица 10.3. Описательная статистика 2018-2019 весенний семестр в SPSS

Описательные статистики . TypeGroup = EG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	9 9	22	67	**41,44**	**14,993**	224,778	0,375	0,717	-0,673	1,400

Описательные статистики TypeGroup = KG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note	22 22	22	71	**43,14**	**13,464**	181,266	0,436	0,491	-0,436	0,953

Приложение 11. Критерий Манна-Уитни результатов уточняющего эксперимента

Анализ результатов итогового тестирования уточняющего эксперимента по критерию Манна-Уитни в SPSS представлен на рисунках

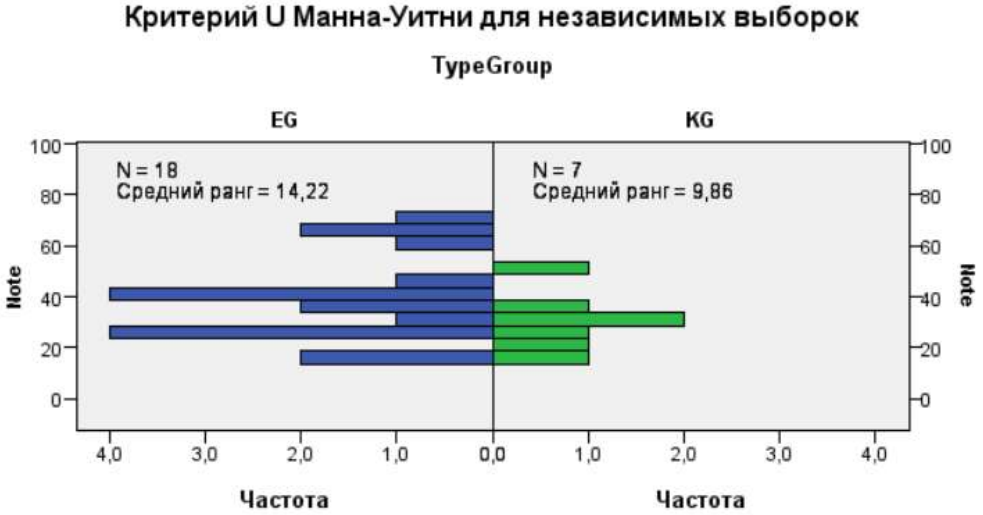
2017-2018 осенний семестр

Итоги по проверке гипотезы

	Нулевая гипотеза	Критерий	Значимость	Решение
1	Распределение Note является одинаковым для категорий TypeGroup.	Критерий U Манна-Уитни для независимых выборок	,198[1]	Нулевая гипотеза принимается.

Выводятся асимптотические значимости. Уровень значимости равен ,05.

[1]Приводится точная значимость критерия.



Всего N	25
U Манна-Уитни	41,000
W Вилкоксона	69,000
Статистика критерия	41,000
Стандартная ошибка	16,497
Стандартизованная статистика критерия	-1,334
Асимптотическая знч. (2-сторонний критерий)	,182
Точная знч. (2-сторонний критерий)	,198

Рис. 11.1. 2017-2018 осенний семестр

Вывод: табличное значение критерия Манна Уитни для 18 и 7 равно 35. Т.к. расчетное больше табличного (41 > 35), то принимается нулевая гипотеза о статистической незначимости различий в средних КГ (30) и ЭГ (39,44)

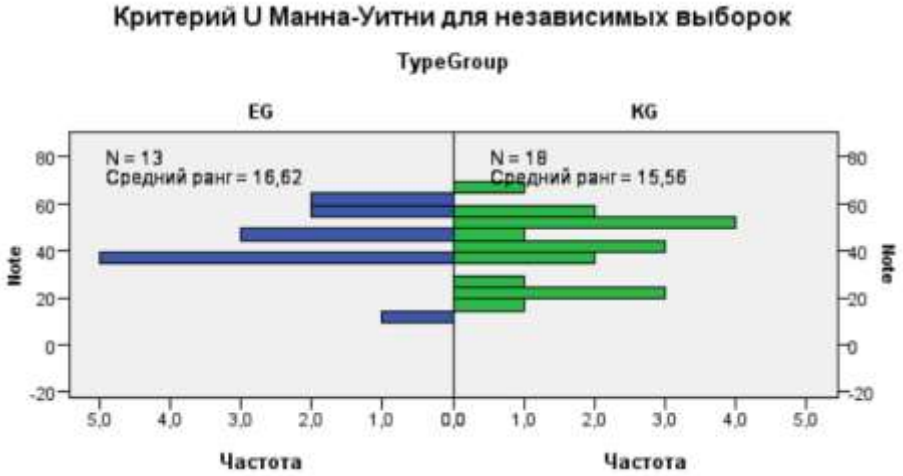
2017-2018 весенний семестр

Итоги по проверке гипотезы

	Нулевая гипотеза	Критерий	Значимость	Решение
1	Распределение Note является одинаковым для категорий TypeGroup.	Критерий U Манна-Уитни для независимых выборок	,767[1]	Нулевая гипотеза принимается.

Выводятся асимптотические значимости. Уровень значимости равен ,05.

[1]Приводится точная значимость критерия.



Всего N	31
U Манна-Уитни	109,000
W Вилкоксона	280,000
Статистика критерия	109,000
Стандартная ошибка	24,940
Стандартизованная статистика критерия	-,321
Асимптотическая знч. (2-сторонний критерий)	,748
Точная знч. (2-сторонний критерий)	,767

Рис. 11.2. 2017-2018 весенний семестр

Вывод: табличное значение критерия Манна Уитни для 18 и 13 равно 75.

Т.к. расчетное значение критерия Манна-Уитни больше табличного (125 > 75), то принимается нулевая гипотеза о статистической незначимости различий в средних КГ (41,89) и ЭГ (44,15) с вероятностью 95%.

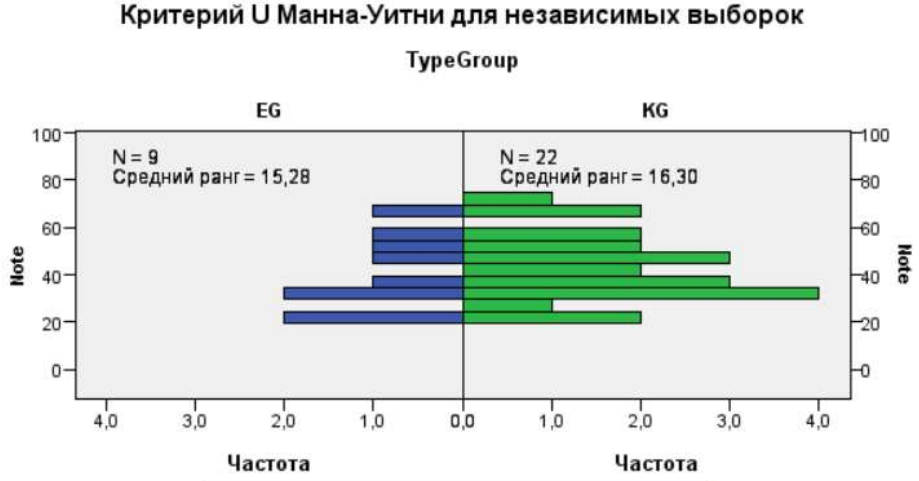
2018-2019 осенний семестр

Итоги по проверке гипотезы

	Нулевая гипотеза	Критерий	Значимость	Решение
1	Распределение Note является одинаковым для категорий TypeGroup.	Критерий U Манна-Уитни для независимых выборок	,781[1]	Нулевая гипотеза принимается.

Выводятся асимптотические значимости. Уровень значимости равен ,05.

[1]Приводится точная значимость критерия.



Всего N	31
U Манна-Уитни	105,500
W Вилкоксона	358,500
Статистика критерия	105,500
Стандартная ошибка	22,923
Стандартизованная статистика критерия	,284
Асимптотическая знч. (2-сторонний критерий)	,777
Точная знч. (2-сторонний критерий)	,781

Рис. 11.3. 2018-2019 осенний семестр

Вывод: табличное значение критерия Манна Уитни для 22 и 9 равно 60

Т.к. расчетное больше табличного (105,5 > 60), то принимается нулевая гипотеза о статистической незначимости различий в средних ЭГ (41,44) и КГ (43,14).

Приложение 12. Описательная статистика формирующего эксперимента

Количественное описание основных статистических показателей результатов итогового тестирования в рамках формирующего эксперимента выполнено средствами SPSS

Таблица 12.1. Описательная статистика 2019-2020 осенний семестр в SPSS

Описательные статистики typeGroup = EG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	3 3	70	77	73,00	3,606	13,000	1,152	1,225	.	.

Описательные статистики[a] typeGroup = KG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	6 6	54	67	61,83	5,269	27,767	-0,721	0,845	-1,324	1,741

Таблица 12.2. Описательная статистика 2019-2020 весенний семестр в SPSS

Описательные статистики . typeGroup = EG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	7 7	68	85	77,57	6,347	40,286	-0,660	0,794	-0,905	1,587

Описательные статистики typeGroup = KG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	17 17	32	73	53,71	11,746	137,971	-,0272	0,550	-0,666	1,063

Таблица 12.3. Описательная статистика 2020-2021 весенний семестр в SPSS

Описательные статистики typeGroup = EG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	10 10	58	93	75,00	11,353	128,889	0,017	0,687	-0,866	1,334

Описательные статистики typeGroup = KG

	N	Минимум	Максимум	Среднее	Стд. отклонение	Дисперсия	Асимметрия		Эксцесс	
	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Статистика	Стд. ошибка	Статистика	Стд. ошибка
Note N	10 10	38	79	60,50	13,890	192,944	-0,437	0,687	-1,124	1,334

Приложение 13. Исходные данные формирующего эксперимента

Таблица. Экранные формы экспериментальных данных в SPSS

2019-2020 осенний семестр

	FIO_stud	Id_stud	Note
1	2020_TI19B...	19ЭГ-1	70
2	2020_TI19V...	19ЭГ-2	72
3	2020_ti19vt_...	19ЭГ-3	77
4	2020_18ПЭ_...	19ЭГ-4	74
5	2020_18ПЭ_...	19ЭГ-5	63
6	2020_38_ЗО...	19КГ-1	65
7	2020_38_ЗО...	19КГ-2	66
8	2020_38_ЗО...	19КГ-3	59
9	2020_38_ЗО...	19КГ-4	57
10	2020_38_ЗО...	19КГ-5	62
11	2020_38_ЗО...	19КГ-6	54

2019-2020 весенний семестр

	FIO_stud	Id_stud	Note	typeGroup
1	2020_ЭД-19_К...	20ЭГ-1	68	1
2	2020_ЭД-19_К...	20ЭГ-2	80	1
3	2020_ЭД-19_К...	20ЭГ-3	85	1
4	2020_ЭД-19_М...	20ЭГ-4	78	1
5	2020_ЭД-19_Н...	20ЭГ-5	70	1
6	2020_ЭД-19_П...	20ЭГ-6	83	1
7	2020_ЭД-19_С...	20ЭГ-7	79	1
8	2020_22_Буши...	20КГ-1	48	2
9	2020_22_Горка...	20КГ-2	41	2
10	2020_22_Екю...	20КГ-3	71	2
11	2020_22_Иван...	20КГ-4	58	2
12	2020_22_Клюк...	20КГ-5	42	2
13	2020_22_Кучук...	20КГ-6	62	2
14	2020_22_Мари...	20КГ-7	53	2
15	2020_22_Мель...	20КГ-8	32	2
16	2020_22_Мися...	20КГ-9	73	2
17	2020_22_Пару...	20КГ-10	36	2
18	2020_22_Пушк...	20КГ-11	60	2
19	2020_22_Ризов...	20КГ-12	43	2
20	2020_22_Сабот...	20КГ-13	61	2
21	2020_22_Семе...	20КГ-14	63	2
22	2020_22_Стрек...	20КГ-15	57	2
23	2020_22_Харчу...	20КГ-16	54	2
24	2020_22_Шуме...	20КГ-17	59	2

2020-2021 осенний семестр

	FIO_stud	Id_stud	Note	typeGroup
1	2021_ТИ20_Б...	ЭГ20о-1	85	1
2	2021_ТИ20_Б...	ЭГ20о-2	93	1
3	2021_ТИ20_Д...	ЭГ20о-3	61	1
4	2021_ТИ20_К...	ЭГ20о-4	87	1
5	2021_ТИ20_М...	ЭГ20о-5	72	1
6	2021_ТИ20_П...	ЭГ20о-6	77	1
7	2021_ТИ20_С...	ЭГ20о-7	58	1
8	2021_ТИ20_С...	ЭГ20о-8	73	1
9	2021_ТИ20_С...	ЭГ20о-9	78	1
10	2021_ТИ20_Т...	ЭГ20о-1	66	1
11	2021_317_Аг...	КГ20о-1	38	2
12	2021_317_Бе...	КГ20о-2	67	2
13	2021_317_Бу...	КГ20о-3	70	2
14	2021_317_Га...	КГ20о-4	53	2
15	2021_317_Го...	КГ20о-5	51	2
16	2021_317_Ло...	КГ20о-6	61	2
17	2021_317_Ло...	КГ20о-7	71	2
18	2021_317_Лу...	КГ20о-8	42	2
19	2021_317_Фр...	КГ20о-9	73	2
20	2021_317_Цу...	КГ20о-1	79	2

Приложение 14. Критерий Манна-Уитни результатов формируюещго эксперимента

Анализ результатов итогового тестирования уточняющего эксперимента по критерию Манна-Уитни в SPSS представлен на рисунках

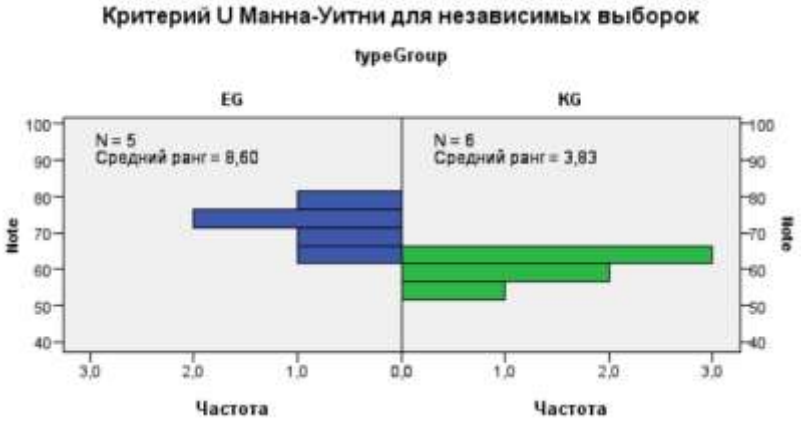
2019-2020 осенний семестр

Итоги по проверке гипотезы

	Нулевая гипотеза	Критерий	Значимость	Решение
1	Распределение Note является одинаковым для категорий typeGroup.	Критерий U Манна-Уитни для независимых выборок	0,0173[1]	Нулевая гипотеза отклоняется.

Выводятся асимптотические значимости. Уровень значимости равен ,05.

[1]Приводится точная значимость критерия.



Всего N	11
U Манна-Уитни	2,000
W Вилкоксона	23,000
Статистика критерия	2,000
Стандартная ошибка	5,477
Стандартизованная статистика критерия	-2,373
Асимптотическая знч. (2-сторонний критерий)	,018
Точная знч. (2-сторонний критерий)	,017

Рис. 2019-2020 осенний семестр

Вывод: Табличное значение критерия Манна Уитни для n_1=5 и n_2=6 на уровне значимости α=0,01 равно 2. Т.к. расчетное значение критерия Манна-Уитни равно 2, то отклоняется нулевая гипотеза о статистической незначимости различий в средних ЭГ (71,2) и КГ (60,5) с вероятностью 99%, т.е. принимается гипотеза H_1.

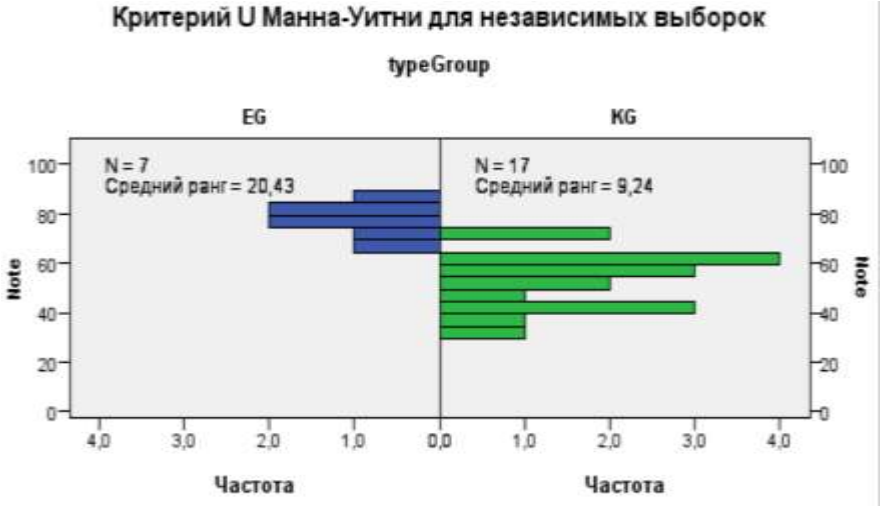
2019-2020 весенний семестр

Итоги по проверке гипотезы

	Нулевая гипотеза	Критерий	Значимость	Решение
1	Распределение Note является одинаковым для категорий typeGroup.	Критерий U Манна-Уитни для независимых выборок	,000[1]	Нулевая гипотеза отклоняется.

Выводятся асимптотические значимости. Уровень значимости равен ,05.

[1]Приводится точная значимость критерия.



Всего N	24
U Манна-Уитни	4,000
W Вилкоксона	157,000
Статистика критерия	4,000
Стандартная ошибка	15,745
Стандартизованная статистика критерия	-3,525
Асимптотическая знч. (2-сторонний критерий)	,000
Точная знч. (2-сторонний критерий)	,000

Рис. 2019-2020 весенний семестр

Вывод: Табличное значение критерия Манна Уитни для n_1=7 и n_2=17 при α=0,01 равно 28. Т.к. расчетное значение критерия Манна-Уитни меньше табличного (4<23), то отклоняется нулевая гипотеза о статистической незначимости различий в средних ЭГ (m_1=77,57) и КГ (m_2=53,71) с вероятностью 99%, т.е. принимается гипотеза H_1.

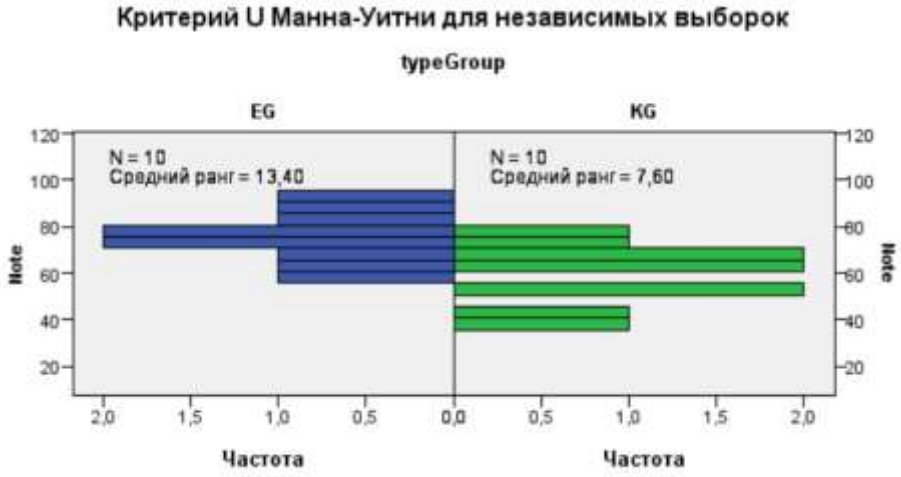
2020-2021 осенний семестр

Итоги по проверке гипотезы

	Нулевая гипотеза	Критерий	Значимость	Решение
1	Распределение Note является одинаковым для категорий typeGroup.	Критерий U Манна-Уитни для независимых выборок	0,0288[1]	Нулевая гипотеза отклоняется.

Выводятся асимптотические значимости. Уровень значимости равен ,05.

[1]Приводится точная значимость критерия.



Всего N	20
U Манна-Уитни	21,000
W Вилкоксона	76,000
Статистика критерия	21,000
Стандартная ошибка	13,219
Стандартизованная статистика критерия	-2,194
Асимптотическая знч. (2-сторонний критерий)	,028
Точная знч. (2-сторонний критерий)	,029

Рис. 2020-2021 осенний семестр

Вывод: Табличное значение критерия Манна Уитни для n_1=10 и n_2=10 при α=0,05 равно 27, при α=0,01 равно 19. Т.к. расчетное значение критерия Манна-Уитни меньше табличного (21<27), то отклоняется нулевая гипотеза о статистической незначимости различий в средних ЭГ (m_1=75,0) и КГ (m_2=59,9) с вероятностью 95%, т.е. принимается гипотеза H_1.

Приложение 15. Расчет φ* — критерия углового преобразования Фишера

Осенний семестр 2019-2020

Критерий φ* — угловое преобразование Фишера

Ограничения: при $n_1, n_2 \geq 5$ возможны любые сопоставления.

Таблица 15.1. Результаты итогового тестирования в осеннем семестре 2019-2020 уч.г.

Экспериментальная группа (ЭГ)	70	72	77	74	63	
Контрольная группа (КГ)	65	66	59	57	62	54

Расчет:

Применяем критерий углового преобразования Фишера для сравнения процента студентов в экспериментальной группе, получивших на итоговом тестировании более 66 баллов, с процентом студентов, получившим такой же результ, в контрольной группе. В экспериментальной группе более 66 баллов набрали 4 человека из 5 (80%), в контрольной – 1 человек из 6 (16,7%).

Сформулируем гипотезы:

H_o: доля студентов набравших более 66 баллов в экспериментальной группе не больше, чем в контрольной группе.

H_1: доля студентов набравших более 66 баллов в экспериментальной группе больше, чем в контрольной группе.

Построим четырехклеточную таблицу эмпирических частот по двум значениям признака «есть эффект (набрал больше 66 баллов)» и «нет эффекта (набрал меньше 66 баллов)».

Таблица 15.2. Четырехклеточная таблица эмпирических частот 2019-2020 осенний семестр

Набран балл	Экспериментальная группа			Контрольная группа		
	Результаты студентов	Количество студентов	Доля	Результаты студентов	Количество студентов	Доля
Больше 66	70 72 74 77	4	**80%**	66	1	**16,7%**
Меньше 66	63	1	20%	54 57 59 62 65	5	83,3%
Итого	356 баллов	n_1=5	100%	363 балла	n_2=6	100%
	Средний балл=71,2			Средний балл=60,5		

Определим величины φ по формулам:

$$\varphi_1(0{,}8) = 2 * \arcsin\sqrt{0{,}8} = 2{,}214$$

$$\varphi_2(0{,}167) = 2 * \arcsin\sqrt{0{,}167} = 0{,}839$$

Проверим по статистическим таблицам величины φ, соответствующие процентным долям в каждой из групп: φ_1(80%)=2,214 и φ_2 (16,7%)=0,839.

Эмпирическое значение φ* вычисляют по формуле: $\varphi * = (\varphi_1 - \varphi_2) * \sqrt{\frac{n_1 * n_2}{n_1 + n_2}}$

где $\varphi_1 -$ угол, соответствующий большей % доле; $\boldsymbol{\varphi_2} -$ угол, соответствующий меньшей % доле; n_1 – количество наблюдений в выборке 1; n_2 – количество наблюдений в выборке 2.

В нашем случае: $\varphi^*_{\text{эмп}} = (2{,}214 - 0{,}839) * \sqrt{\frac{5*6}{5+6}}$=2,27

По таблице уровней статистической значимости **φ*** значению 2,27 соответствует p=0.012.

Критическое значение **φ*** определим по таблицам для уровня значимости p=0.01 и p=0.05: $\varphi^*_{\text{эмп}} = \begin{cases} 1{,}64 \text{ при } p = 0{,}05 \\ 2{,}31 \text{ при } p = 0{,}01 \end{cases}$

Вывод: Т.к. $\varphi^*_{\text{эмп}} > \varphi^*_{\text{крит}}$ (2,27>1.64), то гипотеза Н0 отклоняется с вероятностью 95% и принимается гипотеза Н1 о том, что доля студентов набравших более 66 баллов в экспериментальной группе больше, чем в контрольной группе.

Весенний семестр 2019-2020

Таблица 15.3. Результаты итогового тестирования в осеннем весеннем 2019-2020 уч.г.

Экспериментальная группа (ЭГ)	63	80	85	78	70	83	79										
Контрольная группа (КГ)	48	41	71	58	42	62	53	32	73	36	60	43	61	63	57	54	59

Расчет:

В экспериментальной группе более 66 баллов набрали 6 человека из 7 (85,7%), в контрольной 2 человека из 17 (11,8%).

Сформулируем гипотезы:

H_o: доля студентов набравших более 66 баллов в экспериментальной группе не больше, чем в контрольной группе.

H_1: доля студентов набравших более 66 баллов в экспериментальной группе больше, чем в контрольной группе.

Построим четырехклеточную таблицу эмпирических частот по двум значениям признака «есть эффект (набрал больше 66 баллов)» и «нет эффекта (набрал меньше 66 баллов)».

Таблица 15.4. Четырехклеточная таблица эмпирических частот 2019-2020 весенний семестр

Набран балл	Экспериментальная группа			Контрольная группа		
	Результаты студентов	Количество студентов	Доля	Результаты студентов	Количество студентов	Доля
Больше 66	70, 78, 80 83, 85,79	6	**85,7%**	71 73	2	**11,8%**
Меньше 66	64	1	14,3%	32, 36, 41, 42 43, 48, 53, 54 57, 58, 59, 60 61, 62, 63	15	88,2%
Итого	460 баллов	n_1=7	100%	913 балла	n_2=17	100%
	Средний балл=77			Средний балл=53,71		

По статистическим таблицам определим величины φ*, соответствующие процентным долям в каждой из групп: $\varphi_1(85{,}7\%)=2{,}456$ и $\varphi_2(11{,}8\%)=0{,}701$.

Определим величины φ по формулам:

$$\varphi_1(0{,}857) = 2 * \arcsin\sqrt{0{,}857} = 2{,}456$$

$$\varphi_2(0{,}118) = 2 * \arcsin\sqrt{0{,}118} = 0{,}701$$

Эмпирическое значение: $\varphi * = (\varphi_1 - \varphi_2) * \sqrt{\frac{n_1 * n_2}{n_1 + n_2}} = (2{,}456 - 0{,}701) * \sqrt{\frac{7*17}{7+17}} = 3{,}91$

По таблице уровней статистической значимости **φ*** значению 3,91 соответствует p=0.000. Критическое значение $\varphi^*_{\text{кр}} = \begin{cases} 1{,}64\ (p \le 0{,}05) \\ 2{,}31\ (p \le 0{,}01) \end{cases}$

Вывод: Т.к. $\varphi^*_{\text{эмп}} > \varphi^*_{\text{крит}}$ (3,91>2,31), то гипотеза H_0 отклоняется, и принимается гипотеза H_1 о том, что доля студентов набравших более 66 баллов в экспериментальной группе выше, чем в контрольной группе.

Осенний семестр 2020-2021

Таблица 15.5. Результаты итогового тестирования в осеннем семестре 2020-2021 уч.г.

ЭГ	85	93	61	87	72	77	58	73	78	66
КГ	38	67	70	53	51	61	65	42	73	79

Расчет:

В экспериментальной группе более 66 баллов набрали 8 человек из 10 (80%), в контрольной 4 человека из 10 (40%).

Сформулируем гипотезы:

H_o: доля студентов набравших более 66 баллов в экспериментальной группе не больше, чем в контрольной группе.

H_1: доля студентов набравших более 66 баллов в экспериментальной группе больше, чем в контрольной группе.

Построим четырехклеточную таблицу эмпирических частот по двум значениям признака «есть эффект (набрал 66 баллов и больше)» и «нет эффекта (набрал меньше 66 баллов)».

Таблица 15.6. Четырехклеточная таблица эмпирических частот 2020-2021 осенний семестр

Набран балл	Экспериментальная группа			Контрольная группа		
	Результаты студентов	Количество студентов	Доля	Результаты студентов	Количество студентов	Доля
Больше или равно 66	72, 73, 77, 78, 85, 87, 93, 66	8	**80%**	70, 73, 79, 67	4	**40%**
Меньше 66	58, 61,	2	20%	38, 42, 51, 53, 61, 65	6	60%
Итого	750 баллов	n_1=10	100%	599 баллов	n_2=10	100%
	Средний балл=75,0			Средний балл=59,9		

Определим величины φ, соответствующие процентным долям в каждой из групп, по формулам:

$$\varphi_1(0{,}8) = 2 * \arcsin\sqrt{0{,}8} = 2{,}214$$

$$\varphi_2(0{,}4) = 2 * \arcsin\sqrt{0{,}4} = 0{,}1{,}369$$

Проверим по статистическим таблицам: φ_1(80%)=2,214 и φ_2 (40%)=1,369

Эмпирическое значение φ*: $\varphi * = (\boldsymbol{\varphi}_1 - \boldsymbol{\varphi}_2) * \sqrt{\frac{n_1 * n_2}{n_1 + n_2}}(2{,}214 - 1{,}369) * \sqrt{\frac{10*10}{10+10}} = 1{,}89$

По таблице уровней статистической значимости **φ*** значению 1,89 соответствует p=0.029

Критическое значение **φ*** определим по таблицам для уровня значимости p=0.01 и p=0.05: $\varphi^*_{\text{кр}} = \begin{cases} 1{,}64\ (p \le 0{,}05) \\ 2{,}31\ (p \le 0{,}01) \end{cases}$

Вывод: Т.к. $\varphi^*_{\text{эмп}} > \varphi^*_{\text{крит}}$ (1,89>1,64), то гипотеза H_0 отклоняется, и принимается гипотеза H_1 о том, что доля студентов набравших более 66 баллов в экспериментальной группе выше, чем в контрольной группе.

Приложение 16. Список конференций, в рамках которых представлены результаты диссертационного исследования

1) The 4th Conference of Mathematical Society of the Republic of Moldova, dedicated to the centenary of Vladimir Andrunachievici (1917-1997) (CMSM), June 28 – July 2, 2017, Chişinău
2) III Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", 19-20 квітня 2018 року, Украина, Кропивницький.
3) Conferinţa ştiinţifico-didactică naţională cu participare internaţională "Probleme actuale ale didacticii ştiinţelor reale", ediția a II-a, consacrată aniversării a 80-a a profesorului universitar Ilie Lupu, 11 – 12 mai 2018, Chisinau
4) The 26th Conference on Applied and Industrial Mathematics (CAIM), September 20-23, 2018, Chisinau.
5) Conferință științifică naţională cu participate internaţională "Învătământ superior: tradiţii, valori, perspective", 28-29 septembrie 2018, Chişinău.
6) Международная научно-практическая конференция «Общекультурные и естественнонаучные аспекты образования в интересах устойчивого развития», 25 ноября – 3 декабря 2018,. Арзамас, Россия.
7) The scientific-practical conference with international participation "The use of modern educational and informational technologies for the training of professional competences of the students in higher education institutions", December 7-8, 2018, Balti.
8) Міжнародна науково-практична інтернет-конференція «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації. Вип. 44. Переяслав-Хмельницький, 2019, Україна.
9) Conferinta Republicana a Cadrelor Didactice, 1-2 martie 2019, Universitatea de Stat din Tiraspol, Chisinau.
10) Перший Міжнародний науково-практичний WEB-форум Розбудова єдиного відкритого інформаційного простору освіти впродовж життя, 26–28 березня 2019, Київ-Харків, Україна
11) XXIV Международная научно-методическая конференция «Управління якістю підготовки фахівців», 18-19 квітня 2019 р. Одеса, Україна.
12) Conference on Applied and Industrial Mathematics. CAIM 2019, Targoviste, September 19-22, 2019. Chişinău.
13) Conferința științifica naționala cu participare internaţională „Învățământ Superior: Tradiții, Valori, Perspective". Didactica Ştiinţelor. 27 – 28 septembrie, 2019. Chişinău.
14) Conferinţa ştiinţifico-practice cu participare internaţională „Utilizarea tehnologiilor

educaţionale şi informaţionale moderne pentru formarea competenţelor profesionale ale absolvenţilor instituţiilor de învăţământ superior", 6-7 decembrie 2019. Bălți

15) Науково-практична інтернет-конференція «Економічна кібернетика: теорія, практика та напрямки розвитку», кафедри Економічної кібернетики та інформаційних технологій Одеського національного політехнічного університету, 27-28 листопада 2019. Одеса, Україна.

16) X Всероссийская научно-практическая конференция с международным участием «Экономическая психология инновационного менеджмента», 13 декабря 2018, Брянск, Россия.

17) Conferinta Republicana a Cadrelor Didactice, 28-29 februarie 2020,. Chişinău.

18) II Міжнародний науково-практичний WEB-форум (Forum-SOIS) „Розбудова єдиного відкритого інформаційного простору освіти впродовж життя", 25-27 march 2020. Харьків, Україна.

19) Conferinţa ştiinţifica naţionala cu participare internaţională „Învăţământ superior: tradiţii, valori, perspective", 29-30 septembrie 2020, Chişinău.

20) International Symposium "Actual Problems of Mathematics and Informatics": dedicated to the 90th birthday of professor Ion Valuţă, november 27-28, 2020, Chişinău.

21) Науково-практична інтернет-конференція «Економічна кібернетика: теорія, практика та напрямки розвитку», кафедри Економічної кібернетики та інформаційних технологій Одеського національного політехнічного університету. 24-25 листопада 2020, Одеса**,** Україна.

22) Conferinţa Republicana a Cadrelor Didactice, 27-28 februarie 2021, UST, Chișinău.

23) Conferinţa ştiinţifică cu participare internaţională "învățământul superior: tradiţii, valori, perspective", 1 - 2 octombrie 2021, UST, Chișinău.

24) Conferința științifică internațională „Abordări inter/transdisciplinare în predarea științelor reale, (concept STEAM)"dedicată aniversării a 70 de ani de la nașterea profesorului universitar Anatol Gremalschi. 29 - 30 octombrie 2021, Chișinău.

25) Conferinta Republicana a Cadrelor Didactice, 26-27 februarie 2019, Universitatea de Stat din Tiraspol, Chisinau.

ДЕКЛАРАЦИЯ ОБ ОТВЕТСТВЕННОСТИ

Нижеподписавшийся, заявляю про личную ответственность, что материалы, представленные в докторской диссертации, являются результатом личных научных исследований и разработок. Осознаю, что в противном случае буду нести ответственность в соответствии с действующим законодательством.

Фамилия, имя Богданова Виолетта

Подпись

Число

БЛАГОДАРНОСТЬ

Написание этой докторской диссертации было бы невозможно без помощи замечательных людей вокруг меня, которым глубоко признательна. В первую очередь выражаю самую искреннюю благодарность моему научному руководителю, доктору хабилитат, профессору Кирияк Любомиру. Благодарю за плодотворные отношения, эффективную организацию научного исследования, постоянную заботу и всемерную поддержку, внимание и содействие моему научному росту.

Особая благодарность членам сопроводительной комиссии. Покойному академику, оставившему светлые воспоминания, доктору физико-математических наук Чобану Митрофану за поддержку и теплые напутствия, которые навсегда останутся в моей памяти. Доктору наук Ботнарь Валентине за конструктивные обсуждения и критический анализ самых первых результатов, сопровождаемый ценными рекомендациями. Доктору наук, доценту Глоба Анжеле за теплые слова напутствия и важные советы в части формирования практической части.

Выражаю самую искреннюю признательность официальным оппонентам. Доктору хабилитат, профессору Гремальски Анатолию за важнейшие замечания и бесценные советы, которые помогли усовершенствовать содержательную часть работы. Доктору хабилитат, профессору Охрименко Сергею за внимательное отношение и актуальные рекомендации в области исследования. Доктору Брайкову Андрею за внимательность и тактичность.

Доктору хабилитат, профессору Лупу Илие, за доброжелательное отношение в период обучения в докторантуре и важные рекомендации в процессе подготовки к защите.

Получение научных результатов и их анализ были бы невозможны без прочной научной базы, поэтому я хотела бы сердечно поблагодарить профессорско-преподавательский состав экономического факультета Одесского Национального политехнического университета (Украина) и факультета физики, математики и информатики Тираспольского государственного университета в Кишиневе. За заботливое отношение и за существенную поддержку, глубоко благодарна Администрации Докторальной школы, Университета и коллегам. Я глубоко благодарна своим коллегам кафедры Информатики и информационных технологий за дружескую атмосферу и отзывчивость. Особую благодарность хочу выразить доктору Марии Павел за ценные советы , данные в процессе подготовки диссертационной работы к защите.

Не могу не упомянуть самыми теплыми словами покойного доктора физико-математических наук Георгице Евгения за бесценные советы и мотивацию, благодаря которым оказалась в докторантуре Тираспольского государственного университета.

Спасибо членам моей семьи, которая поддерживала меня все эти годы.

Богданова Виолетта

CURRICULUM VITAE

ФАМИЛИЯ	Богданова
ИМЯ	Виолетта
ГРАЖДАНСТВО	MDA
АДРЕС	MD-2069, Republica Moldova, or. Chişinău, str. Gh. Iablocichin 5
TEL.	.+(373)67257457
E-MAIL:	bogdanovaleta@gmail.com

ОБРАЗОВАНИЕ

1995-2000	Одесский Национальный Политехнический Университет (Украина, г. Одесса) специальность: «Экономическая кибернетика», квалификация магистр
2015-2017	Тираспольский Государственный Университет (г. Кишинэу) специальность «Педагогическое образование» профиль «Информационные технологии обучения» квалификация магистр
2017-2021	Şcoala Doctorală «Ştiinţe ale Educaţiei» a Parteneriatului instituţiilor de învăţământ superior Universitatea de Stat din Tiraspol, Universitatea de Stat „B.P.Haşdeu” din Cahul şi Institutul de Ştiinţe ale Educaţiei. 532.02 – Didactică Şcolară (pe trepte şi discipline de învăţământ) Chişinău, Moldova

КУРСЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

11.11.2008 г. – 29.04.2009 г.	«Пути реализации кредитно-модульной системы организации учебного процесса и тестовых форм контроля знаний» по тематике «Европейские нормы и стандарты организации самостоятельной работы и контроля качества обучения» (146 часов) Одесский Национальный Политехнический Университет (г. Одесса, Украина)
12-23 декабря 2016	«Современные информационные технологии в экономике, управлений и юриспруденции» (72 часа) НОУ ВО «Московская Академия Экономики и Права» (РФ, г. Москва)
2019	"Методы обработки и анализа социологических исследований в программе SPSS" (72 часа). Приднестровский Университет им. Т. Г. Шевченко (Тирасполь, Молдова)
2020	"Использование возможностей системы moodle в высшем образовании" (36 часов). Приднестровский Университет им. Т. Г. Шевченко (Тирасполь, Молдова)
30.01.2022-13.02.2022	«Основы проектной работы» (108 часов). Национальный исследовательский университет «Высшая школа экономики» (РФ, Москва)

ОБЛАСТИ НАУЧНОГО ИНТЕРЕСА

Дидактика информатики; информационная безопасность и защита информации; прикладная информатика в экономике, статистика, информационные технологии в обучении; современные системы оценивания результатов обучения; образовательные приложения для разработки интерактивных учебно-методических материалов.

УЧАСТИЕ В НАЦИОНАЛЬНЫХ И МЕЖДУНАРОДНЫХ НАУЧНЫХ ПРОЕКТАХ

20.80009.0807.20 Proiectului de cercetări ştiinţifice „Metodologia implementării TIC în procesul de studiere a ştiinţelor reale în sistemul de educaţie din Republica Moldova din perspectiva inter/transdisciplinarităţii (concept STEAM)”, inclus în „Program de stat” (2020-2023), Prioritatea IV: Provocări societale, cifrul 20.80009.0807.20, cu suportul financiar oferit de Agenţia Naţională pentru Dezvoltare şi Cercetare

УЧАСТИЕ В НАУЧНЫХ МЕРОПРИЯТИЯХ

2017 1. CMSM 4, 4-ая Конференция математического сообщества Республики Молдова. июнь 28- июль 2, 2017, посвященная столетию со дня рождения Владимира Андрунакевича (1917-1997). Кишинев

2018 2. Conferinţa republicană a cadrelor didactice, 10 марта 2018, UST, Chişinău.

3. III Міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», 19-20 квітня 2018 року, м. Кропивницький (Украина).

4. Научно-дидактическая конференция с международным участием «Актуальные проблемы дидактики фундаментальных наук», II, посвященная 80-летию профессора Илие Лупу, 11-12 мая 2018. Кишинев.

5. CAIM 2018. 26-ая Международная конференция Прикладной и промышленной математики, 20-23 сентября 2018, Кишинев.
6. Conferința științifica naționala cu participare internaţională „Învățământ Superior: Tradiții, Valori, Perspective". 28 – 29 septembrie 2018. UST, Chişinău.

2019
7. Міжнародна науково-практична інтернет-конференція «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації». 28 февраля 2019. Переяслав-Хмельницький (Украина).
8. Conferinţa republicană a cadrelor didactice, 1-2,III. 2019. UST, Chişinău.
9. Перший Міжнародний науково-практичний WEB-форум «Розбудова єдиного відкритого інформаційного простору освіти впродовж життя», 26–28 березня 2019 р. Київ-Харків (Украина).
10. III-ий всероссийский конкурс образовательных web-квестов «Научный поиск» 17 мая 2019 Арзамаский филиал Нижегородского государственного университета (г. Арзамас, Российская Федерация).
11. CAIM 2019. Conference on Applied and Industrial Mathematics, September 19-22, 2019 Targoviste (Romania).
12. Conferința științifica naționala cu participare internaţională „Învățământ Superior: Tradiții, Valori, Perspective". 27-28.X.2019 .UST, Chişinău.
13. Conferinţa ştiinţifico-practice cu participare internaţională "Utilizarea tehnologiilor educaţionale şi informaţionale moderne pentru formarea competenţelor profesionale ale absolvenţilor instituţiilor de învăţământ superior". 6-7 decembrie 2019. Бельцы.

2020
14. Conferinţa republicană a cadrelor didactice, 28-29.II.2020, UST, Chişinău.
15. Второй Міжнародний науково-практичний WEB-форум «Розбудова єдиного відкритого інформаційного простору освіти впродовж життя». 25–27 березня 2020. Київ-Харків, Украина.
16. Conferinta inrenationala "Educatie on-line" sub patronatul Ministerului Educatiei, Culturii si Cercetarii, in parteniriat cu Primaria Municipiul Chisinau, organizat de catre Directia Generala Educatie, Tineret si Sport, 6-11 iulie 2020. Livrarea webinarul interactive cu titlul «Создание образовательного контента средствами платформы Joomag».
17. SIPAMI: International Symposium "Actual Problems of Mathematics and Informatics": dedicated to the 90th birthday of professor Ion Valuţă, 27-28 november 2020, UTM, Chişinău.

2021
18. Conferinţa republicană a cadrelor didactice, 27 -28.II. 2021, UST , Chişinău
19. Conferința științifica naţionala cu participare internaţională "Învăţământ superior: tradiţii, valori, perspective", 1-2 octombrie 2021, UST , Chişinău.
20. Conferința științifică internațională „Abordări inter/transdisciplinare în predarea științelor reale (concept STEAM)", 29-30.X.2021, UST , Chişinău.

2022
21. Conferinţa republicană a cadrelor didactice, 26-27.II.2022, UST , Chişinău

ОПУБЛИКОВАННЫЕ НАУЧНЫЕ РАБОТЫ:

33 научные работы, в том числе:
3 статьи в журналах категории "B" *Acta et commentationes. Ştiinţe ale Educaţiei* и *Revista Univers Pedagogic*,
2 статьи в журналах категории "C" *Revista de Stiinţe Socioumane* и *Acta Et Commentationes* (2018),
1 статья в рецензируемом журнале из списка ВАК РФ *Мир университетской науки: культура, образование*
13 *публикации в материалах* международных научно-методических конференций (2017-2021 гг.).
4 публикации в материалах национальных научно-методических конференций (2018-2022),
7 *публикаций в материалах* национальных научно-методических конференций с международным участием (2018-2021 гг.)

ЯЗЫКОВЫЕ ЗНАНИЯ

Родной язык Русский (уровень C2)
Румынский (уровень C1)
Украинский (уровень C1)
Английский (уровень B1)
Литовский (уровень A1)