

ИЗ ОПЫТА РЕАЛИЗАЦИИ STEM ПРОЕКТА «ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ»

Виолетта БОГДАНОВА, кандидат педагогических наук

<https://orcid.org/0000-0003-4140-6317>

Государственный Педагогический Университет "Ион Крянгэ", Кишинэу, Молдова

Оксана ГРАДИНАРЬ, кандидат педагогических наук

<https://orcid.org/0000-0003-2628-4251>

Государственный Университет им. Алеку Руссо, Бэлць, Молдова

Аннотация. Значительное усложнение и повсеместное применение информационно-коммуникационных технологий, увеличение роста числа кибератак против граждан, общества и государства, являются вызовом для современного общества. Обучение навыкам защиты информации, независимо от уровня образования, становится перманентной задачей для общества.

Во многих странах вопросам обучения информационной безопасности на протяжении всей жизни посвящено множество программ. В данной статье представлен процесс проектирования и реализации STEM проекта по изучению одного из способов обеспечения информационной безопасности, а именно электронно-цифровой подписи. STEM проект организован в форме веб-квеста. В работе проанализированы результаты проекта и формируемые навыки.

Ключевые слова: информационная безопасность, информационно-коммуникационные технологии, дидактические подходы, электронно-цифровая подпись, STEM образование.

FROM THE EXPERIENCE OF IMPLEMENTING THE STEM PROJECT "ELECTRONIC DIGITAL SIGNATURE"

Abstract. The significant complexity and widespread use of information and communication technologies, as well as the increasing number of cyberattacks against citizens, society, and the state, pose a challenge for modern society. The development of information security skills, regardless of the level of education, has become a permanent task for society. In many countries, there are numerous programs dedicated to lifelong information security education. This article presents the process of designing and implementing a STEM project to explore one of the methods of ensuring information security, namely electronic digital signatures. The STEM project is organized in the form of a web quest. The paper analyzes the project's results and the skills that are being developed.

Key words: information security, information-communication technologies, didactic approaches, electronic-digital signature, STEM education.

1. Введение

В настоящее время из-за значительного роста информационных угроз, с которыми сталкиваются все владельцы смартфонов, пользователи социальных сетей, сотрудники различных организаций при работе с информационно-коммуникативными технологиями вопросы обеспечения информационной безопасности становятся важным компонентом современного куррикулума по информатике [1]. С киберугрозами ежедневно сталкиваются, как простые

граждане, так и организации, и государственные органы. Спектр таких угроз постоянно расширяется, что требует перманентного обучения пользователей информационно-коммуникационных технологий навыкам защиты информации и противодействия негативному информационному воздействию. В разных странах вопросам обучения информационной безопасности уделяется много внимания [2,3]. В Республике Молдова в Кодекс об Образовании № CE152/2014 от 17.07.2014 в статье 11 сформулированы образовательные цели:

«(1) Главной образовательной целью является формирование гармоничной личности и развитие системы компетенций, включающей знания, умения, установки и ценности, обеспечивающие возможность активного участия индивида в общественной и экономической жизни.

(2) Образование направлено на формирование следующих ключевых навыков (компетенций):

- a) навыки общения на румынском языке;
- b) навыки общения на родном языке;
- c) навыки общения на иностранных языках;
- d) навыки в математике, науках и технологиях;
- e) навыки в цифровых технологиях;
- f) навык умения учиться;
- g) социальные и гражданские навыки;
- h) навыки предприимчивости и инициативности;
- i) навыки культурного самовыражения и осознания культурных ценностей» [4].

Изучение основ информационной безопасности с позиции STEM обучения согласуется с пунктами d – «навыки в математике, науках и технологиях» и e – «навыки в цифровых технологиях» статьи 11 Кодекса об образовании Республика Молдова.

Данная статья направлена на изучение методов обучения основам информационной безопасности с позиции STEM. Апробация модуля по изучению основ информационной безопасности с применением STEM подхода в группе студентов, обучающихся по специальности среднего профессионального образования «Информационные системы и программирование». Сравнительный анализ результатов обучения в двух группах, обучавшихся по разным методам, позволит определить, какой из подходов эффективен в освоении компетенций в области защиты информации. Исследование поможет педагогам и образовательным учреждениям в повышении качества образования, и адаптации учебного процесса современным вызовам и требованиям.

2. Компетентность в области информационной безопасности

Одним из индикаторов достижений профессиональных компетенций является индикатор достижения «ИДПК-3.1: Способен выявлять, анализировать и оценивать (степень) уровень риска и разрабатывать мероприятия по их минимизации». Данный индикатор уточняет и раскрывает компетенции по пониманию принципов работы, использованию современных информационных технологий и программных средств для решения профессиональных задач, понимания принципов работы современных информационных технологий, а также способности собирать и анализировать информацию.

Дисциплина «Информатика» обладает большим спектром возможностей развития информационно-коммуникационных компетенций необходимых для эффективного обучения, в личной жизни и для будущей профессиональной деятельности. Конкурентные преимущества выпускника в данной области формируются за счет совершенствования навыков поиска, использования и обработки информации, а также развития креативности, критического мышления, умения работать в группе.

При изучении информационной безопасности в профессиональном образовании только как раздела дисциплин информационного цикла, необходимо дать базовые понятия в области защиты информации и ключевые направления защиты.

С позиции информационно-кибернетического подхода [5] в системе понятий в области защиты информации можно выделить две основные подсистемы: угрозы информационной безопасности и средства защиты информации. Изучение источников возникновения угроз, последствий реализации (нарушения целостности, конфиденциальности и доступности), а также формальных и неформальных способов защиты информации, включая организационно-правовые, аппаратно-программные, морально-этические средства защиты позволят сформировать более полное понимание современного ландшафта киберугроз и способов защиты.

Важно разделять уровни возникновения угроз: уровень государства, общества и личности. В зависимости от направления подготовки можно расставлять акценты на новых угрозах, специфичных для конкретных видов профессиональной деятельности. Что касается средств защиты информации, то в полном объеме весь спектр способов защиты, который изучается на соответствующих направлениях подготовки, в рамках одного модуля не представляется возможным изучить.

Данные противоречия приводят к тому, что общесистемное понимание сферы защиты информации позволит сформировать компетенцию по выявлению и определению информационных угроз, оценки степени риска и принятию мер к его

минимизации при работе с информацией в личной жизни и в профессиональной деятельности.

3. Методологические подходы к изучению информационной безопасности в позиции STEM

Эффективным современным дидактическим подходом является применение STEAM подхода в образовательном процессе. В рамках изучения раздела «Информационная безопасность» разработан STEM проект по изучению применению электронно-цифровой подписи для обеспечения идентификации, целостности и юридической значимости цифрового документа. Основные элементы STEM проекта представлены в таблице 1.

Таблица 1. STEM проект «Электронно-цифровая подпись»

Проблема	Электронно-цифровая подпись как средство защиты от нарушения целостности информации	
Сферы применения	Интернет-банкинг Таможенное оформление Государственные услуги Внутренний документооборот предприятия	
Электронная цифровая подпись	(S) Science	Изучение понятий хеш-функций, ассиметричных ключей: открытого и закрытого
	(T) Technology	Использование он-лайн симуляторов создания хеш-значений. Создание программного кода, реализующего хеш-функцию. Подписание текстового файла закрытым ключом. Определение подлинности файла открытым ключом
	(E) Engineering	Проектирование схемы электронного документооборота в организации: кто подписывает документ, где хранятся ключи. Построение UML диаграммы электронного документооборота в организации.
	(M) Mathematics	Простые числа. Операции модульной арифметики. Криптосистемы, используемые в шифровании и алгоритмах электронно-цифровой подписи

Целесообразно вовлекать студентов в реализацию STEM проекта на практических и/или лабораторных занятиях, а также во внеаудиторной (самостоятельной) работе. STEM деятельность может быть организована как краткосрочная (несколько недель), так и долгосрочная (семестр или более) деятельность. Для получения эффективного результата важно спланировать и оказывать методическую поддержку на каждом этапе реализации проекта.

4. Реализация STEM проекта

Для начала студенты должны четко понимать цель и задачи проекта. Работу студентов целесообразно организовать как командную, а не индивидуальную. Таким образом достигается еще один важный навык – умение работать в группе. Рекомендуется сформулировать четкие результаты проекта, которые должны быть достигнуты обучающимися. В таблице 2 приведен пример соотношения цели, деятельности и результатов в рамках STEM проекта по изучению применению электронно-цифровой подписи для обеспечения идентификации, целостности и юридической значимости цифрового документа.

Таблица 2. STEM проект «Электронно-цифровая подпись»

Задание	Деятельность	Результат
(S) Science	Изучение понятий хеш-функций, асимметричных ключей: открытого и закрытого	Схема процесса создания и проверки электронно-цифровой подписи
(T) Technology	Использование он-лайн симуляторов создания хеш-значений. Создание программного кода, реализующего хеш-функцию. Подписание текстового файла закрытым ключом. Определение подлинности файла открытым ключом	Практический опыт работы с электронно-цифровой подписью. Программное приложение по созданию и проверке электронно-цифровой подписи (для студентов, углубленно изучающих информационные технологии)
(E) Engineering	Проектирование схемы электронного документооборота в организации: кто подписывает документ, где хранятся ключи. Построение UML диаграммы электронного документооборота в организации.	Прототип системы безопасности организации
(M) Mathematics	Простые числа. Операции модульной арифметики. Криптосистемы, используемые в шифровании и алгоритмах электронно-цифровой подписи	Решение криптографических задач по созданию и проверке электронно-цифровой подписи

В процессе организации STEM проекта «Электронно-цифровая подпись» для лучшего понимания обучающимися поставленных перед ними задач, можно распределить роли между группами исследователей.

Группа «Ученые» должна изучить теоретические аспекты создания и реализации электронно-цифровой подписи. Если обучающихся в такой группе много, то можно предложить разработать материалы для различных схем создания и проверки электронно-цифровой подписи: RSA и её модификации, Эль-Гамала, ECDSA, DSA, Шнорра, Рабина, GMR.

Группа «Технологи» должна изучить, как работают различные симуляторы электронно-цифровой подписи. Если же проект проводится среди обучающихся по специальности, связанной с информационными технологиями, то им необходимо

будет реализовать проект по созданию и проверке электронно-цифровой подписи на языке программирования высокого уровня.

Группа «Инженеры» должна проанализировать бизнес-процессы организации, внутренний документооборот и построить UML диаграмму текущих бизнес-процессов AS-IS. После анализа слабых мест в безопасности информационных активов и ресурсов организации создать прототип системы безопасности организации.

Группа «Математики» должна изучить математические подходы, применяемые в процессе создания и проверки электронно-цифровой подписи. В результате должен быть подготовлен набор задач с примерами решений.

Для студентов среднего профессионального образования в рамках дисциплины «Информатика» спроектирован и реализован образовательный веб-квест по изучению применения электронно-цифровой подписи с позиции STEM. Веб-квест позволяет организовать проектную деятельность обучающихся с применением современных информационно-коммуникативных технологий [6] для реализации STEM подхода к обучению.

Такой подход позволяет не только стимулировать работу в группе, развивать навыки сотрудничества и коммуникации, но также осваивать учебный материал по индивидуальной образовательной траектории.

Спроектированный веб-квест относится к краткосрочной проектной деятельности, рассчитанной на 2-3 недели. В учебной группе были выделены 4 команды, в каждой был выбран капитан. В течение первой недели студенты подготовили материалы, рассмотрели вместе с педагогом в малых группах. В течение второй недели обучающиеся готовили материалы к представлению результатов исследования. На третьей неделе обучающиеся демонстрировали полученные результаты в рамках семинара-конференции.

Взаимодействие в рамках данного проекта происходило на различных уровнях: студент – студент, студент – учебный материал, студент – преподаватель, студент – информационно-коммуникационные технологии [7].

5. Выводы

Обучение основам кибербезопасности необходимо проводить в течение всей жизни, что обусловлено постоянным усложнением информационно-коммуникационных технологий, увеличением роста числа кибератак, направленных как на общественную инфраструктуру, так и против большого числа обычных граждан.

STEM проекта «Электронно-цифровая подпись» был апробирован в группах среднего профессионального образования в рамках изучения дисциплины

«Информатика». Студенты расширили свои знания в области информационной безопасности, а также развили и усовершенствовали навыки работы с цифровыми технологиями, усовершенствовали навыки публичных выступлений, коммуникаций, креативности и сотрудничества.

Articol realizat în cadrul proiectului de cercetări științifice „Metodologia implementării TIC în procesul de studiere a științelor reale din perspectiva conceptului STEAM și Inteligenței Artificiale”, codul 040101, din cadrul Programului instituțional de cercetare (2024-2027), aprobat prin Ordin MEC nr. 102 din 01.02.2024.

Библиография

1. ENISA Threat Landscape 2025 — ENISA (europa.eu). Disponibil online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
2. Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy') Disponibil online: <https://www.sipotra.it/wp-content/uploads/2023/05/Closing-the-cybersecurity-talent-gap-to-boost-the-EUs-competitiveness-growth-and-resilience.pdf>
3. Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education, November 2021. Disponibil online: <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>
4. Codul Educației al Republicii Moldova № CE152/2014 din 17.07.2014. Disponibil online: <https://www.legis.md/>
5. БОГДАНОВА, В. Информационно-кибернетический подход к проектированию педагогического эксперимента. In: *Revistă de științe socioumane* 48.2, 2021. p. 111-124.
6. DODGE, B. Some Thoughts About WebQuests. 1997. Disponibil online: webquest.sdsu.edu/about_webquests.html.
7. CHIRIAC, L., BOSTAN, M., PAVEL, M., BOGDANOVA, V., JOSU, N. Applying the STEM approach in studying Graph Theory from the perspective of technology-enhanced interactive learning concept. In: *International Conference on Virtual Learning*, 2026. vol. 21, pp. 355-370. <https://doi.org/10.58503/icvl-v21y202631> ISSN 2971-9291.

Recepționat / Received: 17.02.2026

Acceptat / Accepted: 19.03.2026

Email: bogdanova.violeta@upsc.md