

УДК: 004.056.53

АНАЛИЗ МЕЖДУНАРОДНОГО ОПЫТА ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ КИБЕРЗАЩИТЫ

К.К.Сентназаров – доктор технических наук, профессор

Нукусский государственный педагогический институт имени Ажинияза

З.А.Уримбетова – ассистент

Каракалпакский государственный университет имени Бердаха

Таянч сўзлар: киберхима, киберхавфсизлик, таҳлил, таълим, рақамли саводхонлик, компетентлик.

Ключевые слова: киберзащита, кибербезопасность, анализ, образование, цифровая грамотность, компетентность.

Key words: cyber protection, cybersecurity, analysis, education, digital literacy, competence.

Введение. В Узбекистане проблема формирования кибербезопасности в образовательной системе получила широкое признание. Теоретическое исследование кибербезопасности в условиях цифровизации образования имеет международное и национальное значение.

В научных трудах узбекских исследователей, таких как А.Х.Абдукаримов, Ш.З.Хуббиев, У.Турсунотов [1], подчеркивается, что кибербезопасность должна рассматриваться как важная составляющая цифровой грамотности студентов. Национальные стратегии цифровизации («Цифровой Узбекистан – 2030») акцентируют внимание на том, что подготовка специалистов в области информационной безопасности [2].

Актуальность проблемы также отражена в работах международных организаций. ЮНЕСКО и Международный союз электросвязи (ITU) в своих аналитических докладах отмечают, что кибербезопасность является неотъемлемой частью устойчивого развития образования и требует разработки новых методик обучения. В докладе Всемирного экономического форума указывается, что нехватка кадров в области кибербезопасности стала глобальной проблемой, а решение возможно только через интеграцию профильных знаний в систему непрерывного образования.

Образование, являясь одной из ключевых сфер социальной инфраструктуры, оказалось в эпицентре этого процесса. Цифровые технологии, интернет-ресурсы и электронные образовательные платформы стали обязательными инструментами организации учебного процесса, однако одновременно с этим возросла зависимость образовательных систем от цифровой инфраструктуры. Это породило необходимость системной защиты информации. По данным отчёта Всемирного экономического форума (Global Risks Report 2023) [3], киберугрозы стабильно входят в пятёрку наиболее опасных глобальных рисков, а образовательные учреждения всё чаще становятся мишенями атак, что делает вопрос формирования кибербезопасности стратегическим направлением образовательной политики.

Целью статьи является анализ международного опыта стратегии подготовки кадров в области киберзащиты.

Методические подходы к обучению информационной безопасности и Международные стандарты ISO/IEC 27001, NIST Cybersecurity Framework, рекомендации Международного союза электросвязи (ITU) [4], и Европейской комиссии по вопросам киберустойчивости задают ориентиры не только для построения систем защиты информации, но и для подготовки специалистов, в области управления рисками, анализа угроз и обеспечения устойчивости информационных систем. Ведущие университеты мира (MIT, Stanford, ETH Zurich и др.) развивают образовательные программы по кибербезопасности, где ключевым становится междисциплинарный подход: сочетание технических, правовых и гуманитарных дисциплин.

Полученные результаты. Результаты анализа международного опыта стратегии в области киберзащиты показывают, что различные страны мира выстраивают собственные стратегии подготовки кадров в области киберзащиты. Например, в США реализуются инициативы Cybersecurity Education and Training Assistance Program и NICE, направленные на школьников, студентов и педагогов. В Европейском союзе основное внимание уделено внедрению принципов кибербезопасности на всех уровнях образования в рамках Digital Education Action Plan (2021-2027) [5].

В Сингапуре при университетах создаются центры компетенций и исследовательские лаборатории по кибербезопасности. Эти примеры подтверждают, что подготовка специалистов в данной области является мировым трендом.

Стремительное развитие информационно-коммуникационных технологий радикально изменило характер образовательной среды. Если ещё десятилетия назад цифровые ресурсы использовались в качестве вспомогательных средств обучения, то сегодня они составляют основу учебного процесса.

В таблице 1 представлен анализ международного опыта.

1-Таблица. Сравнительный анализ международных инициатив по обучению кибербезопасности

Страна / регион	Образовательные инициативы	Особенности внедрения	Результаты / эффекты
США	SETAP, NICE (нац. программы киберобразования)	Интеграция в школьные и университетские программы	Повышение цифровой грамотности населения
ЕС	Digital Education Action Plan (2021-2027)	Включение основ киберзащиты во все уровни образования	Унификация образовательных стандартов ЕС
Сингапур	Smart Nation, CSA (центры компетенций при вузах)	Создание лабораторий и исследовательских центров	Подготовка кадров для государственного и частного секторов
Узбекистан	Государственные стратегии: «Цифровой Узбекистан — 2030»,	Развитие цифровой экономики и образовательных технологий Создание лабораторий и исследовательских центров	Подготовка кадров для государственного сектора

Результаты, приведенные в таблице показывают, что повышение цифровой грамотности населения, включение основ киберзащиты во все уровни образования и подготовка кадров для государственного и частного секторов имеют приоритетное значение.

Дистанционные технологии, электронные библиотеки, онлайн-курсы и облачные сервисы обеспечивают доступность образования, но в то же время создают новые вызовы в сфере безопасности. В исследовании ЮНЕСКО «Education in a Digital World» (2021) [6] подчеркивается, что цифровизация без системной киберзащиты несёт риски сбоев в образовательном процессе, утраты доверия к онлайн-обучению и нарушения конфиденциальности данных. Современные телекоммуникационные технологии способны не только транслировать знания, но и формировать у школьников и студентов «виртуальную культуру общения и профессионально ориентированный опыт» в условиях цифрового общества. За рубежом: в МГТ студенты проходят обязательные практические курсы на киберполигонах, а в ETH Zurich развиваются исследования в области защиты критической инфраструктуры.

В Узбекистане необходимость формирования кибербезопасности в системе образования имеет особую актуальность. Государственные стратегии, такие как «Цифровой Узбекистан — 2030», ориентированы на развитие цифровой экономики и образовательных технологий, а также на подготовку специалистов, обладающих компетенциями в области защиты информации. В 2022 году был принят Закон Республики Узбекистан «О кибербезопасности» [7], в котором подчеркивается необходимость подготовки кадров для защиты национального информационного пространства. При ведущих университетах страны создаются лаборатории по кибербезопасности и центры компетенций, внедряются новые дисциплины по защите информации.

Узбекские учёные (А.Х.Абдукаримов, Ш.З.Хуббиев [1]) справедливо отмечают, что устойчивое развитие национальной системы образования невозможно без интеграции вопросов киберзащиты в учебные программы и подготовки профессорско-преподавательского состава, владеющего современными методиками.

В области преподавания информационной безопасности всё большее распространение получают компетентностный и деятельностный подходы.

-Компетентностный подход предполагает формирование у студентов не только знаний и умений, но и готовности применять их в реальных ситуациях, что особенно важно в условиях динамично меняющейся цифровой среды.

-Деятельностный подход акцентирует внимание на практических заданиях, проектной деятельности, использовании учебных кейсов и симуляторов кибератак.

Все это позволяет моделировать реальные ситуации информационного противоборства и формировать навыки профессиональной деятельности.

Использование цифровых образовательных технологий.

В последние годы активно развивается концепция blended learning (смешанного обучения), в которой сочетаются традиционные и электронные формы обучения. Применяются виртуальные лаборатории, киберполигоны, облачные образовательные платформы, что создаёт возможность отработки практических навыков в безопасной цифровой среде. Электронные ресурсы и онлайн-курсы позволяют студентам осваивать учебный материал в индивидуальном темпе, а также формируют навык самостоятельной работы и ответственность за результаты обучения. В условиях стремительного роста киберугроз и многообразия информационных технологий требуется использование современных цифровых и интернет-ресурсов, позволяющих обеспечить интерактивность, гибкость и практическую направленность образовательного процесса.

Необходимость формирования кибербезопасности в системе непрерывного образования объясняется совокупностью факторов.

Во-первых, это стремительный рост киберугроз, которые всё чаще затрагивают образовательные организации.

Во-вторых, это глобальная интеграция цифровых технологий в учебный процесс, требующая от студентов и преподавателей компетенций безопасного использования цифровых сервисов.

В-третьих, это мировая нехватка специалистов в области информационной безопасности, устранение которой возможно только через системное включение соответствующих знаний и умений в образовательные программы.

В-четвёртых, это задача формирования общей цифровой культуры, когда каждый гражданин осознаёт риски информационного общества и способен адекватно реагировать на них [8].

С развитием цифровых технологий и интернета социальные сети стали не только местом общения, но и инструментом для распространения информации. Однако, наряду с этим, они также стали площадкой для информационных атак, манипуляций и угроз, которые могут нанести значительный ущерб обществу, компаниям и частным лицам.

Всё это позволяет рассматривать кибербезопасность как стратегическое направление для защиты национального информационного пространства, обеспечивающее устойчивое развитие общества в условиях цифровой трансформации.

Выводы. Зарубежный и отечественный опыт показывает, что успешная подготовка специалистов по информационной безопасности требует междисциплинарности, реализации образовательных программ, включающих изучение криптографии, защиты программного обеспечения, правовых аспектов кибербезопасности и психологии информационного воздействия.

Литература

1. Абдукаримов А.Х., Хуббиев Ш.З., Турсунотов У. Цифровизация и кибербезопасность в системе высшего образования. – Ташкент: «Фан ва технология», 2021.
2. Указ Президента Республики Узбекистан от 5 октября 2020 года № УП-6079 «Об утверждении стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации».
3. Отчёт Всемирного экономического форума. Global Risks Report, 2023.
4. Международные стандарты ISO/IEC 27001, NIST Cybersecurity Framework, рекомендации Международного союза электросвязи (ITU). ISO/IEC 27001:2022 (E).
5. Digital Education Action Plan, 2021-2027.
6. ЮНЕСКО «Education in a Digital World», 2021.
7. Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности».
8. Уримбетова З.А. Информационные угрозы в социальных сетях: взгляд современной молодежи. // Вестник КГУ им. Бердаха. № 2(69), 2025. – С. 219-221.

РЕЗЮМЕ. Мақолада таълим тизимида киберхавфсизликни шакллантириш муаммоси бўйича материаллар тақдим этилган, шунингдек, киберхавфсизлик соҳасида кадрлар тайёрлашда халқаро тажриба таҳлили ҳамда унинг асосларини барча таълим босқичларига киритиш орқали касбий фаолият кўникмаларини моделлаштириш ва шакллантириш масалалари ёритилган.

РЕЗЮМЕ. В статье представлены материалы по проблеме формирования кибербезопасности в образовательной системе, а также приведен анализ международного опыта при подготовке кадров в области киберзащиты и включение ее основ во все уровни образования для моделирования и формирования навыков профессиональной деятельности.

SUMMARY. The article presents materials on the problem of forming cybersecurity in the educational system, and also provides an analysis of international experience in training personnel in the field of cyber protection and the inclusion of its basics in all levels of education for modeling and formation of professional skills.

ОПТИМИЗАЦИЯ УСЛОВИЙ ЛАБОРАТОРНОГО ПОЛУЧЕНИЯ АЦЕТАТА НАТРИЯ ВЫСОКОЙ ЧИСТОТЫ

О.М.Сейтназарова – доктор химических наук (DSc), доцент

Каракалпакский государственный университет имени Бердаха

Ш.А.Кулдашева – доктор химических наук (DSc), профессор

Термезский государственный педагогический институт

А.Б.Абдикамалова – доктор химических наук (DSc), профессор

Институт общей и неорганической химии Академии наук Республики Узбекистан

Ж.Т.Юсупов – стажер-преподаватель

Г.Э.Кувватова – стажер-преподаватель

Каракалпакский государственный университет имени Бердаха

Таянч сўзлар: натрий ацетат, кальций карбонат, мини-технология, лаборатория синтеза, тозалик, pH, ҳарорат.

Ключевые слова: ацетат натрия, карбонат кальция, мини-технология, лабораторный синтез, чистота, pH, температура.

Key words: sodium acetate, calcium carbonate, mini-technology, laboratory synthesis, purity, pH, temperature.

Введение. Ацетат натрия (CH_3COONa) представляет собой соль уксусной кислоты, которая широко применяется в различных областях науки и техники. В аналитической химии он используется для приготовления буферных растворов, стабилизации pH при титриметрических и спектрофотометрических методах анализа. В биотехнологии ацетат натрия применяется как компонент питательных сред, в органическом синтезе – как реагент и промежуточное сырьё для получения органических соединений, а также в пищевой промышленности в качестве консерванта (пищевая добавка E262) [1-3].

Ключевым фактором, определяющим возможность использования ацетата натрия в аналитических и лабораторных исследованиях, является его чистота. Для точных измерений необходим продукт квалификации «химически чистый» (х.ч.) или «чистый для анализа» (ч.д.а.), что требует особых подходов к технологии его получения. В настоящее время значительная часть реагентов высокой чистоты импортируется, что повышает себестоимость аналитических исследований и снижает доступность качественных материалов для научных и учебных лабораторий. В этой связи актуальной задачей является разработка мини-технологий получения таких веществ в условиях, приближённых к лабораторным или полупромышленным [4, 5].

В качестве исходного сырья для синтеза ацетата натрия был выбран карбонат кальция (CaCO_3) квалификации «химически чистый». Это вещество доступно, обладает стабильными свойствами и широко используется в аналитической практике. При взаимодействии с уксусной кислотой (CH_3COOH , ч.д.а.) образуется ацетат кальция, который далее может быть переведён в ацетат натрия с использованием карбоната натрия или гидроксида натрия. Такой подход позволяет не только эффективно утилизировать выделяющийся углекислый газ, но и контролировать чистоту конечного продукта за счёт отделения кальциевых примесей на стадии осаждения [6, 7].

Таким образом, цель настоящей работы заключается в разработке и апробации минитехнологии получения

ацетата натрия высокой чистоты из карбоната кальция х.ч. и уксусной кислоты ч.д.а., с оценкой выхода и качества конечного продукта, а также возможностью применения предложенного процесса в условиях лабораторий высших учебных заведений и научно-исследовательских институтов.

Экспериментальная часть.

Объекты исследования. В качестве исходного сырья использовался карбонат кальция (CaCO_3 , х.ч.), полученный от сертифицированного поставщика химических реактивов. Чистота вещества соответствовала требованиям ГОСТ (массовая доля основного вещества $\geq 99,5\%$, содержание примесей железа $\leq 0,01\%$, тяжёлых металлов $\leq 0,002\%$).

Для проведения реакции применялась уксусная кислота (CH_3COOH , ч.д.а.) с концентрацией $99,8\%$ и дистиллированная вода по ГОСТ 6709–72 ($\text{TDS} \leq 0,1 \text{ мг/л}$). Для стадии замещения кальция использовался карбонат натрия (Na_2CO_3 , х.ч.) или гидроксид натрия (NaOH , ч.д.а.), в зависимости от выбранной схемы.

Вспомогательные реагенты: метилоранж (индикатор для титрования), раствор HCl ($0,1 \text{ моль/дм}^3$) для проверки остаточной щёлочности, этиловый спирт (х.ч.) для промывания осадков и ускорения перекристаллизации.

Оборудование: реактор стеклянный с рубашкой для нагрева (объём 2 л) и механической мешалкой (60–120 об/мин); бюретка на 50 мл (класс точности А) для титриметрического анализа; сушильный шкаф (температурный диапазон 40–300 °С); лабораторный фильтр (нутч-фильтр с вакуумной фильтрацией); аналитические весы (точность $\pm 0,0001 \text{ г}$); pH-метр (диапазон 0–14, точность $\pm 0,01 \text{ pH}$); фотометр для определения следовых примесей.

Методы. Растворение и реакция с уксусной кислотой.

В реактор В1 вносили навеску CaCO_3 (100 г), предварительно диспергированную в 500 мл дистиллированной воды. При постоянном перемешивании порционно добавляли уксусную кислоту (CH_3COOH) до полного растворения кальция и достижения $\text{pH} \approx 6,5\text{--}7,0$. Реакция протекала по уравнению:

