DOI 10.52260/2304-7216.2026.2(63).32
УДК 004.738.5:37.014.5
ГРНТИ 20.23.27

М.Н. Ниязов, PhD[1]
Е.Б. Бейсенгалиев, PhD[1]
А.Т. Мергенбаева, к.э.н., ассоц. профессор[2]
Г.С. Жилкишбаева*, докторант PhD[1]
Esil University, г. Астана, Казахстан[1]
Южно-Казахстанский университет
имени М. Ауезова, г. Шымкент, Казахстан[2]
* – основной автор (автор для корреспонденции)
e-mail: inju202009@mail.ru

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ВУЗОВ: КИБЕРБЕЗОПАСНОСТЬ И ОБЛАЧНЫЕ ТЕХНОЛОГИИ

В статье рассматриваются вопросы управления цифровой трансформацией образовательной среды вузов в условиях требований кибербезопасности и широкого распространения облачных технологий. Переход университетов к облачным моделям организации учебного процесса обнажил уязвимость прежних управленческих решений и поставил защиту информационных ресурсов в число приоритетных задач.

Обоснована необходимость объединения управленческих, технологических и защитных компонентов в единую систему управления цифровой образовательной средой. Отдельно исследуется роль гипервизора: как центральный элемент виртуализированной инфраструктуры он управляет распределением ресурсов и изоляцией сервисов, однако именно он же является наиболее критичной точкой уязвимости. Предложен метод обеспечения кибербезопасности, основанный на мониторинге виртуализированной среды и поведенческом анализе: строится модель штатного функционирования, фиксируются отклонения от нормы, проводится корреляционный анализ событий безопасности, запускаются механизмы автоматического реагирования.

Разработаны математические модели для количественной оценки вероятности обнаружения угроз, уровня аномальной активности, целостности инфраструктуры и результативности системы безопасности. Их применение позволяет перейти от реактивного реагирования на инциденты к их упреждающему выявлению.

Экспериментальная проверка подтвердила работоспособность подхода: по сравнению с традиционными методами зафиксированы более высокая точность обнаружения угроз, меньший уровень ложных срабатываний и сокращенное время реагирования.

Практический результат исследования-интегрированная модель управления цифровой трансформацией образовательной среды вузов, где технологическое развитие, облачные решения и требования кибербезопасности выстроены как единая система, а не конкурируют между собой.

***Ключевые слова**: цифровая трансформация образования, облачные технологии, кибербезопасность, образовательная среда вузов, виртуализация, гипервизор, управление информационной безопасностью.*

***Кілт сөздер:** білім берудің цифрлық трансформациясы, бұлтты технологиялар, киберқауіпсіздік, жоғары оқу орындарының білім беру ортасы, виртуалдандыру, гипервизор, ақпараттық қауіпсіздікті басқару.*

***Keywords:** digital transformation of education; cloud technologies; cybersecurity; higher education environment; virtualization; hypervisor; information security management.*

JEL: I23,O33,D83

Введение. Университеты сегодня оказались перед выбором, которого раньше не было: либо перестраивать управленческую логику под требования цифровой эпохи, либо постепенно утрачивать конкурентоспособность в формирующейся экономике знаний. Университеты переходят к облачным платформам не от хорошей жизни: традиционная ИТ-инфраструктура просто не тянет нагрузки дистанционного обучения и не позволяет оперативно управлять распределенными образовательными ресурсами.

Переход к облаку ставит университеты перед новым классом проблем. Архитектура информационных систем усложняется, а поверхность атак растет. Защитные инструменты прошлого поколения создавались для другой среды-статичной, с фиксированным периметром. Там,

где виртуальные машины динамически создаются и уничтожаются, а границы сети постоянно смещаются, прежняя логика защиты попросту не применима.

Накопленный опыт цифровизации университетов указывает на одну повторяющуюся закономерность: проекты, в которых технологические, управленческие и защитные решения разрабатывались раздельно, а затем «состыковывались», стабильно проигрывают тем, где интеграция была заложена изначально. Особое место в этой конструкции занимает гипервизор-компонент, управляющий виртуальными машинами и распределяющий вычислительные ресурсы. Он же является точкой максимальной концентрации риска: успешная атака на гипервизор открывает доступ ко всей облачной среде одновременно. Именно это обстоятельство диктует необходимость интегрированных подходов к кибербезопасности.

Масштаб проблемы не только технический, но и организационный. Международные исследования в области информационной безопасности фиксируют характерную картину: значительная часть инцидентов в образовательных учреждениях объясняется фрагментарностью защиты. Системы мониторинга, политики доступа и процедуры реагирования функционируют автономно, без единой управленческой логики. В виртуализированной инфраструктуре эта разобщенность порождает слепые зоны. Именно туда, прежде всего на уровень гипервизора, злоумышленники целенаправленно направляют атаки: компрометация этого компонента открывает доступ ко всей среде сразу.

Цель настоящего исследования - разработать интегрированную модель управления цифровой трансформацией образовательной среды вуза, в которой кибербезопасность встроена в управленческую архитектуру как полноправный уровень, а не добавлена поверх готовой системы. Для этого решаются три взаимосвязанные задачи: формализация многоуровневой архитектуры облачной образовательной среды; разработка математических моделей количественной оценки угроз, аномальной активности и целостности системы; экспериментальная проверка подхода по трем критериям-точности обнаружения, частоте ложных срабатываний и времени реагирования.

Обзор литературы. Зарубежные исследователи изучают цифровую трансформацию образования преимущественно в связке с проблемами облачной безопасности-защитой инфраструктур, типологией угроз и архитектурой систем обнаружения атак.

По мнению Oluremi, Vallabhaneni, Lallie и Caporale, облачные вычисления сопряжены с качественно иным профилем угроз: утечки данных, DoS-атаки и компрометация учетных записей требуют превентивных механизмов защиты на основе поведенческого анализа, а не реактивного реагирования по факту инцидента [1]. Pitkar указывает, что автоматизация процессов обнаружения и реагирования с использованием SIEM-, SOAR- и XDR-систем позволяет существенно сократить время выявления инцидентов и снизить нагрузку на службы безопасности [2].

Методологическую базу поведенческого анализа угроз заложили Lee, Stolfo и Mok, разработавшие фреймворк интеллектуального обнаружения вторжений на основе интеллектуального анализа данных [3]. Magklaras и Furnell развили это направление применительно к инсайдерским угрозам, предложив инструментарий оценки вероятности злоупотреблений внутри информационных систем [4]. Применительно к облачным средам оба подхода приобретают особое значение: виртуализация существенно расширяет поверхность атак, прежде всего на уровне гипервизора.

В казахстанской науке эта проблематика разрабатывается с учетом специфики национальной системы образования. Как показывают Nurusheva, Abdiraman, Satybaldina и Goranin, применение алгоритмов машинного обучения в SIEM-системах заметно повышает качество обнаружения аномалий и открывает возможности для автоматизации реагирования на инциденты [5]. По мнению Akhmetov и Seitzhanova, безопасность казахстанских облачных образовательных платформ не обеспечивается одними техническими средствами-организационные меры здесь не менее важны [6]. Tazhibayev и Abdrakhmanov, в свою очередь, фиксируют, что существующие системы кибербезопасности цифровых образовательных платформ в Казахстане не в полной мере учитывают специфику виртуализированных сред [7]. Bernazarova с соавторами отмечают, что цифровая трансформация университетов страны сопряжена с переходом от традиционного ресурсного управления к моделям, основанным на данных и автоматизации процессов [8].

В целом в литературе прослеживается сдвиг от периметровых методов защиты к интеллектуальным системам мониторинга поведения. Однако вопрос о том, как органично

включить кибербезопасность в управленческую модель цифровой трансформации университета, остается в значительной мере открытым.

Основная часть. Облачные технологии стали для университетов рабочей реальностью: учебный процесс, хранение образовательных ресурсов, удаленный доступ к информационным системам-все это уже строится на облачной основе [9]. Облачная образовательная среда (Cloud Learning Environment, CLE) - это программно-аппаратный комплекс, где хранение, обработка и передача данных построены на средствах виртуализации и распределенных вычислений. Ее архитектура многоуровневая. Каждый уровень выполняет собственные функции, и именно характер их взаимодействия в конечном счете определяет и доступность, и защищенность образовательных сервисов [10] (рисунок 1).

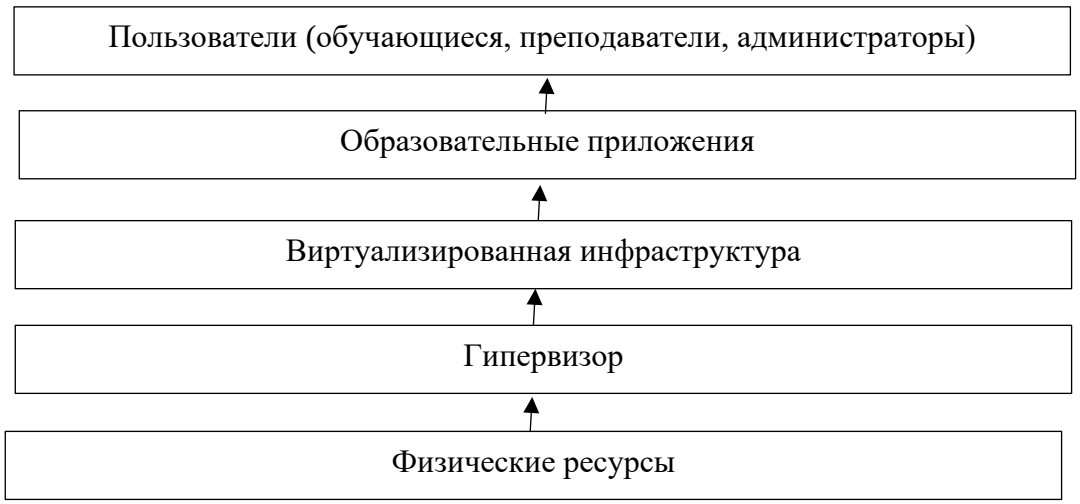

Рисунок – 1. **Многоуровневая архитектура облачной образовательной среды университета**
**Составлен авторами*

Цифровая трансформация университета - это перестройка управленческой логики. Не замена серверов на облачные мощности и не переезд в Zoom. Речь о принципиально ином способе принимать решения, выстраивать учебный процесс, распределять ресурсы. С позиций менеджмента речь идет об управляемом переходе к среде, где технологические и организационные компоненты перестают существовать по отдельности.

На практике это выглядит так: образовательные платформы, облачные сервисы и аналитические инструменты интегрированы между собой, работают на общих политиках безопасности и единых точках контроля доступа. Цифровая экосистема с единой управленческой логикой - не красивая концепция, а рабочая архитектура.

Практика внедрения облачных решений в университетах преподносит один и тот же урок: управленческие решения, принятые в отрыве от технологических и защитных требований, неизбежно порождают уязвимости. Разрыв между ИТ-стратегией и политикой безопасности-это не теоретическая проблема. Это одна из наиболее документированных причин реальных инцидентов в образовательных облачных средах.

Рисунок 1 отражает многоуровневое строение цифровой образовательной среды университета: от физических ресурсов и гипервизора - через виртуализированную инфраструктуру и образовательные приложения - до конечных пользователей: обучающихся, преподавателей и административного персонала.

С управленческой точки зрения каждый из этих уровней требует собственного набора инструментов контроля-единого решения, покрывающего всю архитектуру, не существует (рисунок 2).

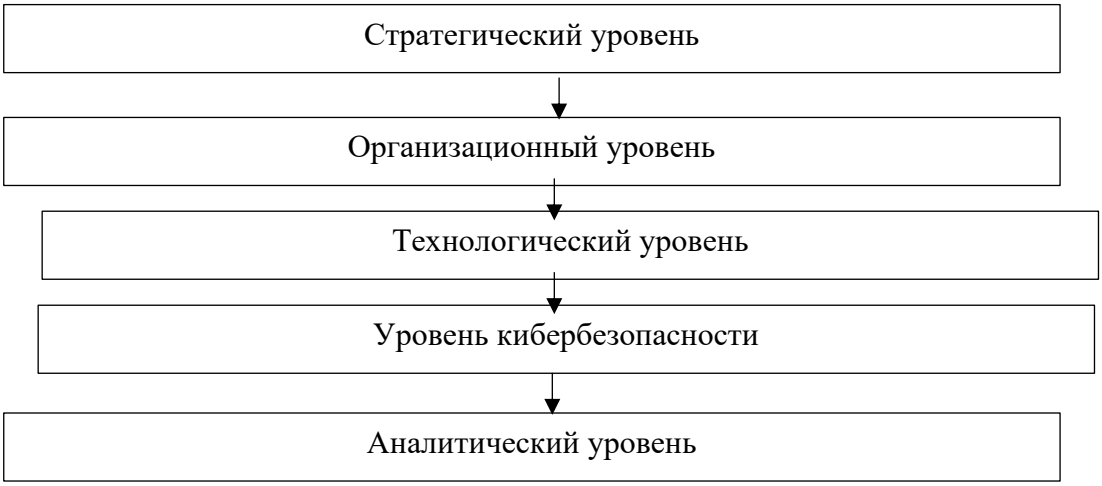

Рисунок – 2. **Иерархическая модель облачной архитектуры**
**Составлен авторами*

На уровне пользователей ключевая задача управления - контроль доступа: кто, когда и к каким ресурсам вправе обращаться. Многофакторная аутентификация и интеллектуальные системы управления доступом давно стали базовым требованием, а не дополнительной опцией. Уровень образовательных приложений требует управления всем жизненным циклом платформ: от выбора и внедрения до интеграции с унаследованной инфраструктурой и текущей поддержки. Уровень гипервизора и физической инфраструктуры имеет особый статус: сбой здесь каскадом затрагивает все вышестоящие уровни сразу, что делает централизованный мониторинг здесь критически необходимым.

Цифровая образовательная среда университета - это иерархически организованная система, в которой решения на каждом уровне влияют на устойчивость остальных. Кибербезопасность в такой архитектуре не может оставаться отдельной функцией ИТ-службы: она встраивается в стратегическое управление университетом.

Логика управления безопасностью меняется фундаментально: от реагирования на уже случившееся - к выявлению угроз до того, как они реализовались. Достигается это через поведенческий анализ среды и распределение защитных механизмов по всем уровням архитектуры - включая те, что традиционно остаются за периметром внимания служб безопасности.

Выбор между IaaS, PaaS и SaaS - не технический, а стратегический. От него зависят и архитектура всей системы, и профиль рисков, с которыми университет будет работать годами. Казахстанские вузы активно применяют облачные решения для дистанционного обучения и управления образовательными ресурсами - и это внедрение уже обнажило новые проблемы: зависимость от провайдеров, болезненную интеграцию с унаследованной ИТ-инфраструктурой, риски утечки данных.

Опыт реализации цифровых стратегий в университетах снова и снова подтверждает одно и то же. Эффективное управление трансформацией возможно только тогда, когда стратегический, организационный, технологический, аналитический уровни и уровень кибербезопасности интегрированы в единую управленческую конструкцию. Не выстроены последовательно - а именно интегрированы. Только в такой архитектуре цифровая среда приобретает реальную устойчивость.

Казахстанские университеты реализуют цифровую трансформацию в контексте государственных программ развития цифровой экономики. Анализ хода их выполнения выявляет устойчивый паттерн: там, где вопросы кибербезопасности не были включены в стратегию с самого начала, а технологические ограничения не учитывались при принятии управленческих решений, трансформация либо буксовала, либо порождала новые уязвимости взамен прежних.

Ценность мониторинга аномальной активности - в его превентивном характере. Показатели выходят за допустимый диапазон раньше, чем угроза оформляется в полноценный инцидент. Именно это временное преимущество и определяет практическую значимость поведенческого анализа.

С позиций информационной безопасности гипервизор занимает особое положение в облачной инфраструктуре. Управление виртуальными машинами и распределение вычислительных ресурсов концентрируются именно здесь - и именно здесь сосредоточен наибольший риск. Атака, достигшая уровня гипервизора, не ограничивается одной виртуальной машиной: под угрозой оказывается вся среда целиком. Часть казахстанских университетов уже отреагировала на эту специфику: в их практику вошли мониторинг поведения виртуальных машин и контроль целостности программной среды.

Эксперименты фиксируют закономерность, которую на практике нередко недооценивают. Эффективность обнаружения угроз определяется не только качеством алгоритмов - в равной мере она зависит от непрерывности наблюдения. Простая формула: выше частота мониторинга - раньше фиксируется вредоносная активность.

Физическая инфраструктура - серверы, каналы связи, системы хранения, центры обработки данных - это фундамент, на котором держатся все цифровые сервисы университета. Сбой здесь отражается на всей среде каскадом. Резервирование мощностей, балансировка нагрузки, автоматизированное восстановление после отказов - все это стандартные инструменты обеспечения устойчивости. Но есть и менее очевидный момент: физическая и информационная безопасность требуют единой системы управления рисками. Раздельное администрирование этих двух областей неизбежно создает слепые зоны.

Здесь, впрочем, есть компромисс, который нельзя игнорировать. Частота мониторинга и вычислительная нагрузка взаимозависимы: чем интенсивнее наблюдение, тем точнее обнаружение, но тем выше потребление ресурсов. Этот баланс нужно закладывать уже на этапе проектирования - потом перестраивать значительно сложнее.

В рамках государственных программ цифровизации казахстанские университеты переходят к управлению, основанному на данных и автоматизации процессов. Практика уже выявила закономерность: там, где технологические, управленческие и защитные решения проектировались вместе с самого начала, трансформация работает. Там, где они вводились порознь и «состыковывались» потом, возникают уязвимости, устранить которые значительно сложнее. Количественная оценка состояния безопасности облачной среды требует формализованных методов. Математическое моделирование позволяет измерять вероятность обнаружения угроз, уровень аномальной активности и результативность защитных механизмов [11], а также прогнозировать сценарии развития кибератак до их реализации [12]. В условиях виртуализации и распределенных вычислений такие модели должны учитывать специфику гипервизоров, виртуальных машин и облачных сервисов - стандартные подходы здесь не работают.

Вероятность обнаружения скрытой угрозы во времени описывается экспоненциальной функцией:

$$Pd(t) = 1 - e^{(-\lambda t)} \quad (1)$$

где *Pd(t)*-вероятность обнаружения угрозы за время наблюдения *t*; *λ*-интенсивность обнаружения угроз системой мониторинга; *t*-время функционирования системы наблюдения.

Модель широко применяется в теории надежности и системах обнаружения вторжений. Ее практический смысл прост: чем дольше работает мониторинг и чем выше λ, тем быстрее система фиксирует вредоносную активность. В облачной образовательной среде значение λ определяется несколькими факторами: частотой опроса гипервизора, качеством алгоритмов обнаружения аномалий, детальностью журналирования системных событий и производительностью аналитической подсистемы. Разница между анализом поведения виртуальных машин каждые несколько секунд и просмотром логов раз в несколько минут - это разница в значении λ на порядок, а значит, и принципиально разное время реакции на угрозу. Опыт казахстанских университетов, внедривших централизованные SIEM-системы, это подтверждает: анализ событий безопасности в реальном времени существенно сокращает время от момента появления угрозы до ее обнаружения.

В образовательном контексте это означает следующее: в периоды пиковой активности — сессия, дистанционный экзамен, массовая загрузка учебных материалов — частота опроса гипервизора должна повышаться автоматически, поскольку именно в эти временные окна вероятность целенаправленных атак на образовательные платформы статистически выше.

Для выявления скрытых угроз в виртуализированных инфраструктурах применяется анализ аномального поведения системы. Интегральный показатель аномальной активности определяется по формуле:

$$A = (1/n) \Sigma |Ri - Bi| \quad (2)$$

где *A* - интегральный показатель аномальной активности; *Ri* - наблюдаемая частота запросов к программному модулю гипервизора; *Bi* - базовое (нормальное) значение активности; *n* - количество анализируемых программных модулей.

Базовое состояние системы устанавливается статистически, по данным о штатной работе виртуальных машин и сервисов в нормальном режиме. Число запросов к базе данных и гипервизору в спокойный период держится в предсказуемом коридоре. Аномальный рост системных вызовов, резкое увеличение обращений к памяти, всплеск сетевых операций-каждый из этих паттернов служит диагностическим сигналом. Через такие отклонения и обнаруживаются rootkit, попытки эскалации привилегий и скрытые процессы внутри виртуальных машин. В казахстанских университетских облачных системах этот подход особенно актуален для обнаружения аномального роста сетевого трафика - одного из ранних признаков DDoS - атаки или распространения вредоносного программного обеспечения по инфраструктуре.

Применительно к образовательным платформам базовое состояние (Bi) устанавливается отдельно для учебного и каникулярного периодов: в сессию число обращений к системе управления обучением (LMS) и серверам хранения учебных материалов закономерно возрастает в несколько раз, и эта динамика должна быть отражена в эталонной модели, иначе система будет генерировать ложные тревоги именно тогда, когда нагрузка на нее наиболее высока.

Третий показатель - коэффициент целостности системы (Is). Он отражает, какая доля программных компонентов инфраструктуры не скомпрометирована.

$$Is = 1 - (Mc / Mt) \quad (3)$$

где *Is* - коэффициент целостности системы; *Mc* - количество скомпрометированных модулей; *Mt* - общее количество программных модулей системы.

Показатель меняется от 0 до 1. Значения, близкие к единице, соответствуют штатной работе; снижение - признак возможного вмешательства. В облачной образовательной среде мониторингу подлежат сервисы образовательных платформ, компоненты гипервизора, системные библиотеки и сетевые сервисы. Инструменты контроля - сравнение хеш - сумм файлов, анализ системных журналов, верификация цифровых подписей, отслеживание изменений в конфигурационных файлах. В ряде казахстанских университетов регулярная проверка целостности серверных файлов уже введена в практику и позволяет своевременно выявлять несанкционированные изменения в программном обеспечении.

Для образовательной среды особую значимость приобретает контроль целостности компонентов LMS, репозиториев учебных материалов и модулей аутентификации: несанкционированное изменение именно этих элементов может повлечь как утечку персональных данных обучающихся, так и фальсификацию результатов оценивания.

Скорость реагирования - параметр, который нередко недооценивают при оценке систем безопасности. Высокая точность обнаружения при медленном реагировании не решает задачи: угроза успевает нанести ущерб. Именно поэтому показатель эффективности реакции (Er) учитывает оба измерения одновременно. Для количественной оценки этого параметра используется следующее выражение:

$$Er = D / Tr \quad (4)$$

где *Er* - показатель эффективности реакции системы безопасности; *D* - точность обнаружения угроз; *Tr* - время реагирования на инцидент.

Основу предложенной системы образует алгоритм выявления скрытых угроз, функционирующий на уровне гостевых операционных систем и гипервизора. Атаки типа rootkit целенаправленно уклоняются от стандартных защитных механизмов, маскируя свое присутствие в системе. Алгоритм отслеживает системные события и характер взаимодействия виртуальных машин с гипервизором - такой подход позволяет фиксировать аномалии на ранних стадиях, когда атака еще не успела развернуться. Проверка метода проводилась на экспериментальном стенде-виртуализированной среде, воспроизводящей типовую облачную инфраструктуру университета. В состав стенда входили несколько виртуальных машин, гипервизор и подсистема мониторинга безопасности. Оценка велась по трем независимым критериям: точности обнаружения угроз (Detection Accuracy), уровню ложных срабатываний (False Positive Rate) и времени реакции (Response Time). В качестве базы для сравнения использовались сигнатурный метод и метод поведенческого анализа(таблица 1).

Таблица –1

Сравнение методов обнаружения угроз

Метод обнаружения	Точность	Ложные срабатывания	Время реакции
Сигнатурный метод	0.72	0.12	8 с
Поведенческий анализ	0.83	0.09	6 с
Предлагаемый метод	0.92	0.05	3 с

**Составлена авторами*

Сигнатурный метод показал точность 0,72-наименьшую из трех. Результат предсказуемый: метод распознает только заранее известные угрозы и не справляется с новыми или измененными вариантами вредоносного кода. Поведенческий анализ улучшил точность до 0,83, однако в динамичной облачной среде-с постоянно меняющейся нагрузкой и активностью пользователей-он генерирует ложные срабатывания в количестве, создающем реальную нагрузку на службу безопасности.

Предложенный метод превзошел оба подхода по всем трем критериям: точность обнаружения-0,92, уровень ложных срабатываний-0,05, время реакции-3 секунды. Такой результат достигается за счет совместного использования мониторинга системных вызовов, поведенческого анализа виртуальных машин и контроля целостности гипервизора-ни один из этих инструментов в отдельности не дает сопоставимого эффекта(таблица 2).

В условиях образовательной среды трехсекундное время реагирования принципиально важно в ситуациях, когда атака происходит в режиме онлайн-экзамена или защиты дипломной работы: даже кратковременный сбой платформы в такой момент несет прямые академические и репутационные последствия для университета.

Таблица – 2

Механизмы защиты на различных уровнях системы

Уровень системы	Тип угрозы	Механизм защиты
Гостевая ОС	Rootkit	Мониторинг поведения
Гипервизор	Эскалация привилегий	Контроль целостности
Сеть	Несанкционированный доступ	Анализ трафика
Приложения	Утечка данных	Контроль доступа

**Составлена авторами*

Таблица 2 наглядно иллюстрирует: каждый архитектурный уровень системы уязвим по-своему и требует собственного механизма защиты. Мониторинг, охватывающий все уровни одновременно, позволяет перехватывать угрозы на разных стадиях их развития и ограничивать распространение вредоносной активности внутри инфраструктуры. Результаты эксперимента подтверждают работоспособность предложенного алгоритма и его применимость в реальных условиях университетских облачных систем.

Обсуждение результатов. Главный результат эксперимента - подтверждение того, о чем часто говорят теоретически, но редко проверяют на практике: мониторинг на уровне гипервизора выявляет вредоносную активность, которую стандартные средства защиты попросту не видят. Логика стандартных систем безопасности - работа на уровне операционной системы или приложений. Rootkit и подобные угрозы именно поэтому туда и не идут. Мониторинг на уровне виртуализации закрывает эту слепую зону: взаимодействие гостевых систем с гипервизором контролируется независимо от того, что происходит внутри самих виртуальных машин.

Ограничения сигнатурных методов в динамичной среде хорошо известны [13]. Они распознают только то, для чего уже написан шаблон - а при нынешней скорости появления новых модификаций вредоносных программ это попросту недостаточно. Поведенческий анализ работает точнее, но в облачной среде с постоянно меняющейся нагрузкой и активностью пользователей он генерирует ложные срабатывания. Каждое такое срабатывание - это нагрузка на службу безопасности и потеря доверия к системе.

Предложенный метод сочетает поведенческий анализ с мониторингом системных вызовов на уровне гипервизора. Это сочетание дает точность обнаружения 0,92 при уровне ложных

срабатываний 0,05 и времени реакции 3 секунды. Быстрая изоляция скомпрометированной виртуальной машины критически важна: именно скорость реагирования определяет, останется ли инцидент локальным или распространится по всей инфраструктуре.

По мере того как растут пользовательская аудитория и объемы обрабатываемых данных, защита облачной инфраструктуры перестает быть сугубо технической задачей и приобретает полноценное управленческое измерение. Полученные результаты подтверждают практическую применимость мониторинга гипервизора и поведенческого анализа виртуальных машин в реальных условиях университетских систем.

Заключение. Ключевой тезис представленной работы состоит в следующем: управленческие механизмы, технологические решения и системы защиты информации, спроектированные раздельно, неизбежно порождают уязвимости на стыках. Устойчивая цифровая образовательная среда возможна только тогда, когда все три компонента изначально выстраиваются как единая система.

Обнаружение скрытых угроз обеспечивается за счет совмещения мониторинга гипервизора с поведенческим анализом виртуализированной среды. Четыре математические модели дают количественную основу для оценки состояния безопасности: вероятность обнаружения угроз, уровень аномальной активности, целостность инфраструктуры, эффективность реагирования. Ни поведенческий анализ, ни мониторинг гипервизора в отдельности таких результатов не дают-эффект возникает именно от их совместной работы в единой управленческой модели.

Экспериментальная проверка дала конкретные числа: точность обнаружения угроз 0,92, уровень ложных срабатываний 0,05, время реакции 3 секунды. Ни один из сравниваемых методов этих показателей не достиг.

Область применения-университетские информационные системы, облачные образовательные платформы, центры обработки данных. Важная практическая характеристика: защищенность образовательных ресурсов повышается без существенного роста вычислительной нагрузки.

Следующий шаг-интеграция метода с алгоритмами машинного обучения. Это позволит перейти к адаптивной настройке порогов обнаружения под конкретную инфраструктуру и снизить зависимость системы от ручной калибровки.

Статья подготовлена в рамках научного исследования по теме: «Влияние искусственного интеллекта на рынок труда: анализ возможностей и вызовов для молодежи в условиях цифровой трансформации» (по гранту Комитета науки Министерства образования и науки Республики Казахстан; ИРН AP 26105089).

ЛИТЕРАТУРА

1. Oluremi D., Vallabhaneni R., Lallie H., Caporale G.M. Cloud Computing and Cybersecurity: Emerging Threats and Defense Mechanisms. – 2025.

2. Pitkar H. Cloud Security Automation Through Symmetry: Threat Detection and Response // Symmetry. – 2025. – №6(17). – 859 p. – DOI: 10.3390/sym17060859.

3. Lee W., Stolfo S., Mok K. A Data Mining Framework for Adaptive Intrusion Detection. – 1999.

4. Magklaras G., Furnell S. Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse // Computers & Security. – 2002. – №21. – P. 62–73. – DOI: 10.1016/S0167-4048(02)00109-8.

5. Nurusheva A., Abdiraman A.S., Satybaldina D., Goranin N. Machine Learning Algorithms in SIEM Systems for Enhanced Detection and Management of Security Events // Bulletin of L. Gumilyov Eurasian National University. Mathematics, Computer Science, Mechanics Series. – 2024. – №3(148). – P. 6–17. – DOI: 10.32523/bulmathenu.2024/3.1.

6. Ахметов Б.С., Сейтжанова А.К. Методы обеспечения информационной безопасности облачных образовательных платформ // Вестник КазНУ. Серия информационных технологий. – 2022. – №3. – С. 45–52.

7. Тажибаев Т.А., Абдрахманов Е.К. Проблемы кибербезопасности цифровых образовательных платформ в Казахстане // Вестник Евразийского национального университета. – 2021. – №4. – С. 112–119.

8. Bernazarova R., Belgibayeva A., Konbayeva K., Valiyeva S. The Evolution of University Resource Management in Digital Kazakhstan // Вестник Казахского университета экономики, финансов и международной торговли. – 2025. – №4(61). – DOI: 10.52260/2304-7216.2025.4(61).24.

9. Mell P., Grance T. The NIST Definition of Cloud Computing // NIST Special Publication 800-145. – 2011. – DOI: 10.6028/NIST.SP.800-145.

10. Sultan N. Cloud Computing for Education: A New Dawn? // International Journal of Information Management. – 2021. – №56. – Art. 102314.

11. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. – 2021. – P. 305–316.

12. Buczak A., Guven E. A Survey of Data Mining and Machine Learning Methods for Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2021. – №2(23). – P. 1153–1176.

13. Kim G., Lee S., Kim S. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection and Signature-Based Detection // Future Generation Computer Systems. – 2022. – №128. – P. 168–178. – DOI: 10.1016/j.eswa.2013.08.066.

REFERENCES

1. Oluremi D., Vallabhaneni R., Lallie H., Caporale G.M. Cloud Computing and Cybersecurity: Emerging Threats and Defense Mechanisms. – 2025.

2. Pitkar H. Cloud Security Automation Through Symmetry: Threat Detection and Response // Symmetry. – 2025. – №6(17). – 859 p. – DOI: 10.3390/sym17060859.

3. Lee W., Stolfo S., Mok K. A Data Mining Framework for Adaptive Intrusion Detection. – 1999.

4. Magklaras G., Furnell S. Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse // Computers & Security. – 2002. – №21. – P. 62–73. – DOI: 10.1016/S0167-4048(02)00109-8.

5. Nurusheva A., Abdiraman A.S., Satybaldina D., Goranin N. Machine Learning Algorithms in SIEM Systems for Enhanced Detection and Management of Security Events // Bulletin of L. Gumilyov Eurasian National University. Mathematics, Computer Science, Mechanics Series. – 2024. – №3(148). – P. 6–17. – DOI: 10.32523/bulmathenu.2024/3.1.

6. Akhmetov B., Seitzhanova A. Metody obespecheniya informacionnoj bezopasnosti oblachnyh obrazovatel'nyh platform [Methods of information security for cloud educational platforms] // Vestnik KazNU. Seriya informacionnyh tekhnologij. – 2022. – №3. – S. 45–52. [in Russian]

7. Tazhibayev T., Abdrakhmanov E. Problemy kiberbezopasnosti cifrovyh obrazovatel'nyh platform v Kazahstane [Cybersecurity problems of digital educational platforms in Kazakhstan] // Vestnik Evrazijskogo nacional'nogo universiteta. – 2021. – №4. – S. 112–119. [in Russian]

8. Bernazarova R., Belgibayeva A., Konbayeva K., Valiyeva S. The Evolution of University Resource Management in Digital Kazakhstan // Вестник Казахского университета экономики, финансов и международной торговли. – 2025. – №4(61). – DOI: 10.52260/2304-7216.2025.4(61).24.

9. Mell P., Grance T. The NIST Definition of Cloud Computing // NIST Special Publication 800-145. – 2011. – DOI: 10.6028/NIST.SP.800-145.

10. Sultan N. Cloud Computing for Education: A New Dawn? // International Journal of Information Management. – 2021. – №56. – Art. 102314.

11. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. – 2021. – P. 305–316.

12. Buczak A., Guven E. A Survey of Data Mining and Machine Learning Methods for Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2021. – №2(23). – P. 1153–1176.

13. Kim G., Lee S., Kim S. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection and Signature-Based Detection // Future Generation Computer Systems. – 2022. – №128. – P. 168–178. – DOI: 10.1016/j.eswa.2013.08.066.

Ниязов М.Н., Бейсенгалиев Е.Б., Мергенбаева А.Т., Жилкишбаева Г.С.

ЖОҒАРЫ ОҚУ ОРЫНДАРЫНЫҢ БІЛІМ БЕРУ ОРТАСЫН ЦИФРЛЫҚ ТРАНСФОРМАЦИЯЛАУ: КИБЕРҚАУІПСІЗДІК ЖӘНЕ БҰЛТТЫҚ ТЕХНОЛОГИЯЛАР

Аңдатпа

Мақалада жоғары оқу орындарының білім беру ортасын цифрлық трансформациялау үдерісін киберқауіпсіздік талаптары мен бұлттық технологиялардың кеңінен енгізілуі жағдайында басқару мәселелері қарастырылады. Университеттердің оқу үдерісін ұйымдастырудың бұлттық модельдеріне көшуі бұрынғы басқару шешімдерінің осал тұстарын айқындап, ақпараттық ресурстарды қорғауды басым міндеттердің біріне айналдырды.

Білім беру ортасын басқарудың басқарушылық, технологиялық және қорғаныс компоненттерін бірыңғай цифрлық басқару жүйесіне біріктірудің қажеттілігі негізделген. Сонымен қатар гипервизордың рөлі жан-жақты зерттелген: ол виртуалдандырылған инфрақұрылымның негізгі элементі ретінде ресурстарды бөлуді және сервистерді оқшаулауды басқарады, алайда дәл осы компонент ең маңызды осалдық нүктесі болып табылады. Виртуалдандырылған ортаны мониторингтеу мен мінез-құлықтық талдауға негізделген киберқауіпсіздікті қамтамасыз ету әдісі ұсынылған: жүйенің қалыпты жұмыс істеу моделі құрылады, қалыпты жағдайдан ауытқулар тіркеледі, қауіпсіздік оқиғаларына корреляциялық талдау жүргізіледі және автоматты әрекет ету тетіктері іске қосылады.

Қауіптерді анықтау ықтималдығын, аномальды белсенділік деңгейін, инфрақұрылымның тұтастығын және қауіпсіздік жүйесінің тиімділігін сандық бағалауға арналған математикалық модельдер әзірленген. Оларды қолдану қауіпсіздік инциденттеріне реактивті жауап беруден оларды алдын ала анықтау тәсіліне көшуге мүмкіндік береді.

Эксперименттік тексеру ұсынылған тәсілдің тиімділігін растады: дәстүрлі әдістермен салыстырғанда қауіптерді анықтау дәлдігі жоғарылаған, жалған іске қосылулар саны азайған және әрекет ету уақыты қысқарған.

Зерттеудің практикалық нәтижесі – жоғары оқу орындарының білім беру ортасын цифрлық трансформациялауды басқарудың интеграцияланған моделі. Бұл модельде технологиялық даму, бұлттық шешімдер және киберқауіпсіздік талаптары бір-бірімен бәсекелеспей, бірыңғай жүйе ретінде қарастырылады.

Niyazov M., Beisengaliev E., Mergenbaeva A., Zhilkishbaeva G.

DIGITAL TRANSFORMATION OF THE HIGHER EDUCATION ENVIRONMENT: CYBERSECURITY AND CLOUD TECHNOLOGIES

Annotation

This article examines the management of the digital transformation of the higher education environment under the requirements of cybersecurity and the widespread adoption of cloud technologies. The transition of universities to cloud-based models of educational process management has exposed the limitations of traditional management approaches and made the protection of information resources one of the highest priorities.

The study substantiates the need to integrate managerial, technological, and security components into a unified digital educational environment management system. Particular attention is paid to the role of the hypervisor. As the core component of a virtualized infrastructure, it manages resource allocation and service isolation; however, it also represents the most critical point of vulnerability. A cybersecurity approach based on virtualized environment monitoring and behavioral analysis is proposed. The approach involves constructing a model of normal system operation, detecting deviations from baseline behavior, performing correlation analysis of security events, and initiating automated response mechanisms.

Mathematical models have been developed to quantitatively assess the probability of threat detection, the level of anomalous activity, the integrity of the infrastructure, and the overall effectiveness of the security system. Their application enables a shift from reactive incident response to proactive threat detection.

Experimental validation confirmed the effectiveness of the proposed approach. Compared with conventional methods, it demonstrated higher threat detection accuracy, a lower false-positive rate, and reduced response time.

The practical outcome of the study is an integrated management model for the digital transformation of the higher education environment, in which technological development, cloud solutions, and cybersecurity requirements are aligned within a unified system rather than treated as competing priorities.