https://doi.org/10.31489/2024Ped1/106-113

УДК 378.1

МРНТИ 14.15.15 Получена: 17 октября 2023 г. | Одобрена для публикации: 10 января 2024 г.

Ж.О. Жилбаев[1], Д.Б. Абыкенова[1], А.Ж. Асаинова[1*], Ж.Н. Матенова[2], Г.М. Абильдинова[3]

[1]Павлодарский педагогический университет имени А. Маргулана, Павлодар, Казахстан;
[2]Торайгыров Университет, Павлодар, Казахстан;
[3]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан
([*]Корреспондирующий автор. E-mail: assainovaa@ppu.edu.kz)

ORCID: 0000-0003-1868-1142, 0000-0002-0980-8722, 0000-0003-0909-9767,
0000-0001-7457-3811, 0000- 0000-0001-9054-6549

Комплаенс-менеджмент и управление рисками кибербезопасности в системе школьного образования: теоретический обзор

Риск потери персональных данных или кражи важных личных и организационных данных делает кибербезопасность главной проблемой, с которой сталкиваются организации, особенно школы. Целью данной статьи является теоретический обзор исследований в области комплаенс-менеджмента в управлении рисками кибербезопасности в школьной среде, проведенных в период с 2019 по 2023 год, включенных в международную базу данных *Google Scholar*. С помощью описательной методологии представлены значимые данные для определения рисков кибербезопасности школьной среды и механизмов комплаенс-менеджмента системы школьного образования в области кибербезопасности, которые применяются в школах. Анализ данных показал, что в качестве основных рисков кибербезопасности в школе являются социальная инженерия; фишинг; скимминг; угрозы, связанные с технологиями; утечка / потеря данных; нарушения конфиденциальности; угрозы, связанные с домогательствами; инсайдерство; мошенничество с целью компроментации; захват учетной записи; вторжения в онлайн-классы и школьные собрания; недостаточный уровень обеспечения политики безопасности; недостаточная подготовка учителей в сфере кибербезопасности. Школами предпринимаются шаги для предотвращения подобных инцидентов, одним из которых является комплаенс-менеджмент кибербезопасности, включающий механизмы стандартизации процесса кибербезопасности, внедрение политики кибербезопасности в школе, самооценка и оценка мер кибербезопасности. Одним из важнейших механизмов обеспечения соответствия требований кибербезопасности в системе школьного образования является обучение процессу и инструментам кибербезопасности учителей, сотрудников, администрации школы, родителей.

Ключевые слова: кибербезопасность системы школьного образования, комплаенс-менеджмент, управление рисками, теоретический обзор, библиометрическая база данных, конфиденциальность школьных данных, стандартизация процесса кибербезопасности, политика кибербезопасности.

Введение

Большая часть мира сейчас находится в киберпространстве. В результате возросшей зависимости от Интернета кибербезопасность стала одной из важнейших проблем, стоящих перед школами в XXI веке. Зависимость от сложной технологической инфраструктуры имеет свою цену: принимая Интернет так широко, школы подвергли себя целому ряду кибератак со стороны целого ряда правонарушителей, которые ищут школьные данные и информации.

Правительства, предприятия и школы стали жертвами кибератак, киберпреступлений и кибersбоев. Несмотря на повышенное внимание и возросший уровень инвестиций в кибербезопасность, количество киберинцидентов, связанные с ними затраты и их влияние на здоровье людей, продолжает расти [1; 268].

На протяжении первых лет использования технологий человеческий фактор оставался неисследованным и неоспоримым. Однако участившиеся кибератаки, утечка данных и атаки программ-вымогателей часто являются результатом ошибок, допущенных человеком; фактически исследователи указывают, что до 95 % всех киберинцидентов связаны с поддержкой человека [2; 60]. Кибербезопасность — это, по сути, взаимодействие человека и автоматизации, поэтому и машина, и человек потенциально уязвимы. Результаты исследования показывают, что наибольшей уязвимостью в системе безопасности является недостаточная осведомленность сотрудников [3; 11]). Хотя инструменты и технологии

важны, люди являются наиболее важным элементом стратегии кибербезопасности. Первичный анализ состояния школьной среды показывает неосведомленность ее субъектов в вопросах кибербезопасности, киберзащиты и киберэтики [4; 184].

Осенью 2022 года в Казнете увеличилось количество кибератак в несколько сотен раз, были зафиксированы массированные внешние атаки. Это показывает уязвимость сетевых ресурсов и необходимость защиты образовательной среды, так как школы используют информационные системы *Kundelik.kz, bilimland.kz, ekitap.kz, onlinemektep.kz.* Также участившиеся инциденты киберопасности свидетельствуют о наличии в школьной среде проблем, связанных с киберэтикой, кибербуллингом, конфиденциальностью данных, киберзащитой от вирусов, а также о фактах передачи логинов, повторного исправления баллов в электронном журнале и прочие.

Одним из механизмов соблюдения требования кибербезопасности в учреждении является комплаенс-менеджмент, обеспечивающий соответствие требованиям стандарта кибербезопасности в школьной среде. В Казахстане комплаенс-менеджмент — новое явление, особенно это касается школ, где процедуры комплаенс управления еще не внедрены. Поэтому целью данной статьи является теоретический обзор научных исследований по проблеме комплаенс-менеджмента кибербезопасности в школьной среде. Мы определили следующие исследовательские вопросы:

- Какие риски кибербезопасности школьной среды существуют?
- Какие механизмы комплаенс-менеджмента системы школьного образования в области кибербезопасности применяются в школах?

Материалы и методы

Для поиска ответов на исследовательские вопросы был использован метод теоретического обзора научных исследований в базе данных Google Scholar, опубликованных в период с 2019 по 2022 годы.

Теоретический обзор проводился в пять этапов: постановка вопроса или цели поиска, определение стратегии поиска, выбор релевантных научных публикаций, анализ и синтез данных [5; 4]. В качестве поискового запроса была выбрана фраза: «school cybersecurity» AND compliance.

Найдено 28 источников, из которых были отобраны семь публикаций, максимально соответствующих следующим критериям: публикация написана на английском языке; содержание публикации соответствует предмету исследования, включающего процедуры обеспечения соответствия кибербезопасности. Были исключены работы, связанные с образованием в области кибербезопасности в образовательных учреждениях. В следующем разделе представлен количественный и качественный анализ найденных исследований.

Следует отметить, что исследований по теме комплаенс-менеджмента кибербезопасности школьной среды не так много, что свидетельствует о слабом освещении данной проблемы в научной литературе.

Результаты и обсуждение

Отвечая на вопрос: «Какие риски кибербезопасности школьной среды существуют?» были проанализированы отобранные исследования на описание выявленных рисков в школьной среде.

Сфера образования является наиболее уязвимой в области кибербезопасности. По данным исследования [6; 1], сектор образования признан в 2018 году наименее безопасным с наибольшим количеством уязвимостей. Онлайн-обучение только способствовало усугублению данной ситуации. В 2020 календарном году было зафиксировано рекордное количество публично раскрытых инцидентов кибербезопасности в школах.

В исследовании говорится о различного рода кибератаках на школьные ресурсы. Приведено несколько примеров кибератак, которые были зафиксированы за последние 5 лет: фишинг, распределенные атаки «отказ в обслуживании», атака с компрометацией деловой электронной почты, DDoS-атака, атаки с помощью программ-вымогателей.

Как утверждают авторы M. Torres, A. Mullins, N. Thompson, недостаток ресурсов и внимания показывает, что школы являются легкой мишенью для проникновения, часто они медленно реагируют и не обладают необходимыми знаниями для устранения угроз кибербезопасности. В отчете отмечается рост числа атак программ-вымогателей и излагаются технические планы действий по устранению связанных с ними рисков. Ученые также утверждают, что в большей степени к киберопасности приводят человеческие ошибки: ошибочное принятие решений из-за недостаточной подготовки и восприятия угроз, слабая организационная культура безопасности, фишинг, социальная инженерия, вредоносное

программное обеспечение, несоблюдение требований и недостаточный уровень политики безопасности [4, 186; 7, 3].

К типам киберсобытий, влияющих на кибербезопасность школы, исследователи M. Richardson и другие относят технические риски, связанные с технической системой кибербезопасности, утечку данных, риски, связанные с незаконным или неподходящим контентом, угрозы, связанные с домогательствами, такие как киберзапугивание, кибер-преследование и риск раскрытия информации (дети раскрывают свою личную информацию посредством фишинга или обмена информацией на платформах социальных сетей) [8; 32].

В образовательной системе часты случаи мошенничества с платежными картами, раскрытие конфиденциальной информации, взлом или вредоносное программное обеспечение, потеря данных, инсайдерство, порча веб-сайта и социальных сетей, вторжения в онлайн-классы и школьные собрания [9, 17; 10, 12–13].

Важными рисками, которые необходимо учесть при следовании политике кибербезопасности являются киберзапугивания, расстройства, связанные с интернет-играми, рискованное поведение в Интернете, кибер-агрессия и кибер-сплетни [11; 11]. В таблице 1 представлен обобщенный список рисков, рассмотренных в анализируемых исследованиях.

Таблица 1

Риски кибербезопасности в системе школьного образования

Риски	Исследования
Социальная инженерия	M. Torres, M.N. Sadiku, J.B. Ulven
Фишинг / скимминг	M. Torres, E. Belastock, M.D. Richardson, J. B.Ulven
Угрозы, связанные с технологиями	M. Torres, E. Belastock E., M.D. Richardson, T. White
Утечка / потеря данных	M.N.Sadiku, M.D. Richardson, T.L. White
Нарушения конфиденциальности	M.D. Richardson
Угрозы, связанные с домогательствами (киберзапугивание, кибер-преследование, киберагрессия)	I. Diana , M.D. Richardson
Инсайдерство	J.B. Ulven
Мошенничество с целью компроментации	T. White, J.B. Ulven
Захват учетной записи	J.B. Ulven
Вторжения в онлайн-классы и школьные собрания	T. White
Недостаточный уровень обеспечения политики безопасности	M. Torres
Недостаточная подготовка учителей в сфере кибербезопасности	M.N. Sadiku

Ответом на второй исследовательский вопрос: «Какие механизмы комплаенс-менеджмента системы школьного образования в области кибербезопасности применяются в школах?» стал анализ исследований на описание мер обеспечения кибербезопасности в школьной среде для обеспечения соблюдения требований.

Одним из основных мер исследователи E. Belastock, M. Torres считают соблюдение политики кибербезопасности, включающее:

- повышение осведомленности о необходимости принятия мер кибербезопасности;
- разработка и внедрение нормативных актов по кибербезопасности;
- регулирование доступа цифровых устройств к школьным ресурсам;
- фильтрация на шлюзе электронной почты;
- обновление антивирусного программного обеспечения и использование антивирусного решения с централизованным управлением [6; 7].

Риск потери персональных данных или кражи важных личных и/или организационных данных делает кибербезопасность главной проблемой, с которой сталкиваются организации, особенно школы. Поэтому школы должны проявлять инициативу в оценке потенциала слабых мест в их системах кибербезопасности и разработке альтернатив для максимального снижения рисков.

Школы располагают конфиденциальными данными об учениках, родителях, выпускниках, преподавателях и персонале. Записи обычно хранятся спустя десятилетия после того, как учащиеся покидают учебное заведение. Более того, сам объем потенциально ценных данных, хранящихся в

большинстве школ, как правило, делает их весьма привлекательными объектами. Отсутствие централизованной структуры для обеспечения кибербезопасности школы могут размещать свои данные во многих разных местах, а не в одном централизованном местоположении. Данные об учащемся могут храниться отдельно в каждой школе и могут быть объединены централизованно в районном офисе. Данные об учениках и финансовые данные могут храниться отдельно. Эта децентрализованная структура может предоставить киберпреступникам больше возможностей для использования уязвимостей в разрозненных системах, содержащих конфиденциальные данные.

Комплаенс-менеджмент основывается на плане кибербезопасности, включающем обучение сотрудников и учеников, развитие доверия к процедурам кибербезопасности, план соблюдения политики [8; 36].

Политика устанавливает обязательные руководящие принципы, влияющие на благоприятное поведение организации при использовании систем или работе с данными. Все политики информационной безопасности должны соответствовать миссии и целям школы и подчеркивать их. Они создаются для обмена протоколами безопасности, распределения четких ролей и обязанностей и предоставления сотрудникам рекомендаций по обеспечению безопасного поведения во время выполнения своих обязанностей. Роли, обязанности и руководящие принципы также дают ясность в отношении того, с кем следует связаться и как обрабатываются инциденты информационной безопасности.

Некоторые ученые сошлись во мнении, что необходима непрерывная программа, направленная на обеспечение информационной безопасности [8, 38; 9, 35]. Разработка адаптированных стандартов кибербезопасности для школьной системы образования, включая инструменты самооценки кибербезопасности [10; 22].

Предотвращение киберрисков означает стратегический подход к предотвращению киберугроз. План предотвращения молодежных киберрисков, таких как проблемы с убийствами и кибервиктимизация среди старшеклассников заключается в ознакомлении с эмоциональными компетенциями, чтобы исключить многозадачность в средствах массовой информации, кибер-сплетни и фаббинг. Также ученики должны быть осведомлены о своей конфиденциальности при обмене личными данными. Родительское руководство также важно и должно быть частью плана действий по защите учащихся от киберрисков. Предотвращение киберрисков должно быть хорошо спланировано, чтобы учащиеся могли с удовольствием пользоваться Интернетом в киберпространстве, не беспокоясь о кибератаках [11; 14].

На основании теоретического обзора исследований определены основные механизмы комплаенс-менеджмента системы школьного образования в области кибербезопасности, которые применяются в школах (табл. 2).

Таблица 2

Механизмы комплаенс-менеджмента

Механизмы	Исследования
Стандартизация	E. Belastock, M. Sadiku, T. White
Внедрение политики кибербезопасности	I. Diana, T. White
Самооценка и оценка мер кибербезопасности	M. Torres, M. Richardson , T. White
Обучение кибербезопасности учителей, сотрудников, администрации школы, родителей	M. Torres, E. Belastock, M. Sadiku, I. Diana, J. Ulven

Определение рисков кибербезопасности и механизмов комплаенс-менеджмента в школьной среде позволяет проанализировать систему кибербезопасности в школах и содействовать внедрению политики комплаенс-контроля в систему школьного образования Казахстана. Информационная безопасность в Казахстане регулируется концепцией «Киберщит Казахстана», описывающей меры по обеспечению кибербезопасности. Тем не менее в данном документе не описаны конкретные процедуры обеспечения соответствия информационной безопасности принятым нормам. Правительством Республики Казахстан утверждены единые требования в области ИКТ и обеспечения информационной безопасности, перечень необходимых процедур и документов, включающий методику оценки рисков информационной безопасности; правила идентификации, классификации и маркировки активов, инвентаризации и паспортизации средств вычислительной техники и др. Принят ряд документов, регулирующих кибербезопасность для банковской и страховой сферы [12]. Данные документы и процедуры не адаптированы для школьной среды.

В школах генерируются большие объемы данных по отслеживанию успеваемости учащихся, выполнению административных функций, кадрового обеспечения и построению учебного плана. Однако все эти данные не попадают под действие школьных правил по кибербезопасности при услугах третьих сторон интернета. Поэтому зачастую не оценивается предполагаемый риск онлайн ресурсов, у школьников и учителей мало знаний об опасности использования сторонних сервисов [9; 5], педагоги не готовы обучать школьников кибербезопасности [6; 7]. Поэтому для казахстанских школ необходимы политики и руководства по организации цифровой безопасности на всех уровнях, стандарты эффективности в структуре проверки школ для защиты и поддержки учащихся и учителей. Большое значение при этом имеет комплаенс-менеджмент, который позволяет урегулировать нормативно-правовую документацию в области кибербезопасности школ [2; 61], использовать комплекс инструментов и процессов для обеспечения соблюдения правил [3; 26].

Анализ источников позволил определить алгоритм комплаенс-менеджмента по кибербезопасности [1, 270; 2, 60]:

1) единая стратегия для вовлечения — все стейкхолдеры должны понимать важность комплаенса для кибербезопасности школьной среды;

2) оценка рисков — обеспечивает основу для определения действий по предотвращению, смягчению или устранению рисков;

3) аудит политики — инвентаризация инструментов, которые уже существуют в школах;

4) обучение субъектов образовательного процесса для обеспечения кибербезопасности, киберзащиты и киберэтики;

5) механизмы контроля и проверки — обеспечивают соответствие выполнения стандарта кибербезопасности школьной среды и дальнейшую поддержку;

6) подотчетность — это обеспечивает четкие дисциплинарные руководящие принципы и протоколы, подлежащие активному и последовательному применению при несоблюдении норм кибербезопасности.

Теоретический обзор исследований позволил определить ряд рисков кибербезопасности школьной среды, которые важно учитывать при комплаенс-менеджменте системой кибербезопасности в школе.

Заключение

Данное исследование направлено на выявление необходимости комплаенс-менеджмента кибербезопасности системы школьного образования через определение рисков, которым подвергаются школы в информационном пространстве. Включение образовательных учреждений в киберпространство привлекает большое количество злоумышленников за персональными данными учеников, сотрудников школ, недостаточный уровень знаний по кибербезопасности влечет ошибки сотрудников, повышающих уязвимости кибербезопасности школьной среды.

Теоретический обзор показал основные риски, с которыми сталкиваются школы: социальная инженерия, фишинг / скимминг, угрозы, связанные с технологиями, утечка / потеря данных, нарушения конфиденциальности, угрозы, связанные с домогательствами (киберзапугивание, кибер-преследование, кибер-агрессия), инсайдерство, мошенничество с целью компроментации, захват учетной записи, вторжения в онлайн-классы и школьные собрания, недостаточный уровень обеспечения политики безопасности, недостаточная подготовка учителей, школьников, администрации, сотрудников в сфере кибербезопасности.

Для превенции рисков и обеспечение соответствия требованиям кибербезопасности системы школьного образования в проанализированных исследованиях описаны механизмы комплаенс-менеджмента кибербезопасности, такие как механизмы стандартизация процесса кибербезопасности, внедрение политики кибербезопасности в школе, самооценка и оценка мер кибербезопасности. Одним из важнейших механизмов обеспечения соответствия требованиям является обучение процессу и инструментам кибербезопасности учителей, сотрудников, администрации школы, родителей. Данные процедуры отразились в алгоритме комплаенс-менеджмента по кибербезопасности.

Теоретический обзор показал, что количество научных исследований в области комплаенс-менеджмента кибербезопасности системы школьного образования является скудным, что указывает на актуальность проводимого исследования.

Данная статья подготовлена в рамках проекта «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP19678646).

Список литературы

1 Yusif S. Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework / S. Yusif, A. Hafeez-Baig // Journal of Applied Security Research. — 2023. — Vol. 18, No. 2. — P. 267–288. DOI: https://doi.org/10.1080/19361610.2021.1989271.

2 Harris M.A. Promoting cybersecurity compliance [Electronic resource] / M.A. Harris, R. Martin // Cybersecurity education for awareness and compliance. — IGI Global, 2019. — P. 54–71. — Access mode: https://www.igi-global.com/chapter/promoting-cybersecurity-compliance/225917.

3 Vasileiou I. Cybersecurity education for awareness and compliance [Electronic resource] / I. Vasileiou, S. Furnell (Eds.). IGI Global, 2019. — 305 p. — Access mode: https://www.igi-global.com/book/cybersecurity-education-awareness-compliance/210239.

4 Sadiku M.N.O. Cybersecurity for Education [Electronic resource] / M.N.O. Sadiku, U.C. Chukwu, J.O. Sadiku // European Journal Of Innovation in Nonformal Education. — 2023. — Vol. 3, No. 6. — P. 182–188. — Access mode: http://www.inovatus.es/index.php/ejine/article/view/1828/1831.

5 Kitchenham B. Guidelines for performing systematic literature reviews in software engineering [Electronic resource] / B. Kitchenham, S. Charters. — 2007. — Access mode: https: //www.elsevier.com/data/promis_misc/525444systematicreviews-guide.pdf.

6 Belastock E. Our Biggest Nightmare Is Here [Electronic resource] / E. Belastock // Education Next. — 2022. — Vol. 22. — No. 2. — Access mode: https://go.gale.com/ps/.

7 Torres M. Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector [Electronic resource] / M. Torres, A. Mullins, N. Thompson // ACIS 2022 Proceedings. — 2022. — 96. — P. 1–10. — Access mode: https://aisel.aisnet.org/acis2022/96/.

8 Richardson M.D. Planning for Cyber Security in Schools: The Human Factor [Electronic resource] / M.D. Richardson et al. // Educational Planning. — 2020. — Vol. 27, No. 2. — P. 23–39. — Access mode: https://eric.ed.gov/?id=EJ1252710.

9 Ulven J.B. A systematic review of cybersecurity risks in higher education / J.B. Ulven, G. Wangen // Future Internet. — 2021. — Vol. 13, No. 2. — P. 1–40. DOI: https://doi.org/10.3390/fi13020039.

10 White T. About the K12 Security information exchange: Annual report [Electronic resource] / T. White. — 2022. — 30 p. — — Access mode: https://info.identityautomation.com/hubfs/PDFs/StateofK12Cybersecurity2022.pdf.

11 Diana I. Cyber Risk among High School Students: A Thematic Review / I. Diana, I.A. Ismail, M. Zairul // Malaysian Journal of Social Sciences and Humanities (MJSSH). — 2023. — Vol. 8, No. 4. — P. 1–19. DOI: https://doi.org/10.47405/mjssh.v8i4.2251.

12 Постановление Правительства Республики Казахстан Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности / 20 декабря 2016 года № 832. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P1600000832.

Ж.О. Жилбаев, Д.Б. Абыкенова, А.Ж. Асаинова, Ж.Н. Матенова, Г М. Абильдинова

Мектептегі білім беру жүйесіндегі комплаенс-менеджмент және киберқауіпсіздік тәуекелдерін басқару: теориялық шолу

Дербес деректерді жоғалту немесе маңызды жеке және ұйымдық деректерді ұрлау қаупі киберқауіпсіздікті ұйымдардың, әсіресе мектептер осындайға тап болса, онда басты мәселенің бірі болмақ. Мақаланың мақсаты халықаралық Google Scholar дерекқорына енгізілген, 2019 және 2023 жылдар аралығында өткізілген, яғни мектеп ішінде киберқауіпсіздік тәуекелдерін басқарудағы комплаенс-менеджмент саласындағы зерттеулерге теориялық шолу жасау. Сипаттамалық әдіснаманың көмегімен мектеп ішіндегі киберқауіпсіздік тәуекелдерін және мектептерде қолданылатын киберқауіпсіздік саласының мектептегі білім беру жүйесінің комплаенс-менеджмент тетіктерін анықтау үшін маңызды деректер келтірілген. Деректерді талдау көрсеткендей, мектептегі киберқауіпсіздіктің негізгі қауіптері әлеуметтік инженерия, фишинг, скимминг, технологияға байланысты қауіптер, деректердің бұзылуы/жоғалуы, құпиялылықтың бұзылуы, зорлық-зомбылыққа байланысты қауіптер, инсайдерлік, ымыраға келу мақсатында алаяқтық, есептік жазбаны тартып алу, онлайн сабақтар мен мектеп жиналыстарына басып кіру, қауіпсіздік саясатын қамтамасыз етудің жеткіліксіз деңгейі, киберқауіпсіздік саласында мұғалімдерді даярлаудың жеткіліксіздігі. Мектептер мұндай оқиғалардың алдын алу бойынша шаралар қабылдауда, олардың бірі киберқауіпсіздік процесін стандарттау, мектептің киберқауіпсіздік саясатын іске асыру, өзін-өзі бағалау және киберқауіпсіздік шараларының бағалау тетіктерін қамтитын киберқауіпсіздікті сәйкестендіру менеджменті. Мектептегі білім беру жүйесінде киберқауіпсіздік талаптарының сақталуын қамтамасыз етудің маңызды тетіктерінің бірі мұғалімдерді, қызметкерлерді,

мектеп әкімшілігін және ата-аналарды киберқауіпсіздік үдерісі мен құралдарына оқыту болып табылады.

Кілт сөздер: мектептегі білім беру жүйесінің киберқауіпсіздігі, комплаенс-менеджмент, тәуекелдерді басқару, теориялық шолу, библиометриялық дерекқор, мектеп деректерінің құпиялылығы, киберқауіпсіздік процесін стандарттау, киберқауіпсіздік саясаты.

Zh.O. Zhilbayev, D.B. Abykenova, A.Zh. Assainova, Zh.N. Matenova, G.M. Abildinova

Compliance management and cybersecurity risk management in the school education system: a theoretical review

The risk of personal data loss or theft of important personal and organizational data makes cybersecurity a major problem faced by organizations, especially schools. The purpose of this article is a theoretical review of research in the field of compliance management in cybersecurity risk management in the school environment, conducted in the period from 2019 to 2023, included in the Google Scholar international database. With the help of a descriptive methodology, significant data are presented to determine the cybersecurity risks of the school environment and the compliance management mechanisms of the school education system in the field of cybersecurity that are used in schools. Data analysis has shown that the main cybersecurity risks at school are social engineering, phishing, skimming, threats related to technology, data leakage/loss, privacy violations, threats related to harassment, insider trading, fraud for the purpose of compromise, account hijacking, intrusions into online classrooms and school meetings, insufficient level of security policy, insufficient training of teachers in the field of cybersecurity. Schools are taking steps to prevent such incidents, one of which is cybersecurity compliance management, which includes mechanisms for standardizing the cybersecurity process, implementing a cybersecurity policy at school, self-assessment and evaluation of cybersecurity measures. One of the most important mechanisms for ensuring compliance with cybersecurity requirements in the school system is teaching the process and tools of cybersecurity to teachers, staff, school administration, parents.

Keywords: cybersecurity of the school education system, compliance management, risk management, theoretical review, bibliometric database, confidentiality of school data, standardization of the cybersecurity process, cybersecurity policy.

References

1 Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework. *Journal of Applied Security Research*, *18*(2), 267–288. https://doi.org/10.1080/19361610.2021.1989271.

2 Harris, M.A., & Martin, R. (2019). Promoting cybersecurity compliance. In *Cybersecurity education for awareness and compliance* (pp. 54–71). IGI Global. Retrieved from https://www.igi-global.com/chapter/promoting-cybersecurity-compliance/225917.

3 Vasileiou, I., & Furnell, S. (Eds.). (2019). Cybersecurity education for awareness and compliance. IGI Global. Retrieved from https://www.igi-global.com/book/cybersecurity-education-awareness-compliance/210239.

4 Sadiku, M.N.O., Chukwu, U.C., & Sadiku, J.O. (2023). Cybersecurity for Education. *European Journal of Innovation in Nonformal Education*, 3(6), 182–188. Retrieved from http://www.inovatus.es/index.php/ejine/article/view/1828/1831.

5 Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Retrieved from https://www.elsevier.com/data/promis_misc/525444systematicreviewsguide.pdf.

6 Belastock, E. (2022). Our Biggest Nightmare Is Here. *Education Next*, *22*(2). Retrieved from https://go.gale.com/ps/.

7 Torres, M., Mullins, A., & Thompson, N. (2022). Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector. *ACIS 2022 Proceedings*, 96, 1–10. Retrieved from https://aisel.aisnet.org/acis2022/96/.

8 Richardson, M.D. et al. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23–39. Retrieved from https://eric.ed.gov/?id=EJ1252710.

9 Ulven, J.B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 1–40. https://doi.org/10.3390/fi13020039.

10 White, T. (2022). About the K12 Security information exchange: Annual report. Retrieved from https://info.identityautomation.com/hubfs/PDFs/StateofK12Cybersecurity2022.pdf.

11 Diana, I., Ismail, I.A., & Zairul, M. (2023). Cyber Risk among High School Students: A Thematic Review. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *8*(4), 1–19. https://doi.org/10.47405/mjssh.v8i4.2251.

12 (2016). Postanovlenie Pravitelstva Respubliki Kazakhstan «Ob utverzhdenii edinykh trebovanii v oblasti informatsionno-kommunikatsionnykh tekhnologii i obespecheniia informatsionnoi bezopasnosti» [The Government of the Republic of Kazakhstan On the approval of uniform requirements in the field of information and communication technologies and information security. Resolution No. 832 of December 20, 2016. Retrieved from https://adilet.zan.kz/rus/docs/P1600000832 [in Russian].

Information about authors

Zhilbayev, Zh.O. — Candidate of pedagogical sciences, Professor, Acting Chairman of the Board, Rector of Pavlodar Pedagogical University named after A. Margulan, Pavlodar, Kazakhstan;

Abykenova, D.B. — PhD, Associate Professor, Pavlodar Pedagogical University named after A. Margulan; Pavlodar, Kazakhstan;

Assainova, A.Zh. — Candidate of pedagogical sciences, Associate Professor; Director of the Center for Pedagogical Research, Pavlodar Pedagogical University named after A. Margulan, Pavlodar, Kazakhstan;

Matenova, Zh.N. — Master of pedagogical sciences, Head of Compliance Service, Toraigyrov University, Pavlodar, Kazakhstan;

Abildinova, G.M. — Candidate of pedagogical sciences, Associate Professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.