Министерство науки и высшего образования
Республики Казахстан
Южно-Казахстанский педагогический университет
имени Өзбекәлі Жәнібеков

Жилбаев Ж.О., Абыкенова Д.Б., Асаинова А.Ж.,
Сырымбетова Л.С., Кульшарипова З.К.

# ПЕДАГОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ШКОЛЬНОЙ СРЕДЫ С ИСПОЛЬЗОВАНИЕМ КОМПЛАЕНС-МЕНЕДЖМЕНТА

Монография

Павлодар, 2025

УДК 004.056.5:373.5
ББК 32.973:74.20

Рекомендовано Ученым советом Южно-Казахстанского педагогического университета имени Өзбекәлі Жәнібеков (протокол №2 от 24.09.2025 г.).

**Рецензенты**:
Жетписбаева Б.А. – д.п.н., профессор Astana IT University

Мухамедиева К.М. – доктор PhD, ассоциированный профессор НАО «Павлодарский педагогический университет имени Әлкей Марғұлан»

Кажиакпарова Ж.С. – к.п.н., ассоциированный профессор кафедры «Физическая культура и информатика» Западно-Казахстанского инновационно-технологического университета

П24 **Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента:** Монография/Жилбаев Ж.О., Абыкенова Д.Б., Асаинова А.Ж., Сырымбетова Л.С., Кульшарипова З.К. – Павлодар: РИО, 2025. – 134 с.

ISBN 978-601-267-831-4

В коллективной монографии рассматриваются теоретические и практические аспекты педагогического обеспечения кибербезопасности школьной среды с использованием механизмов комплаенс-менеджмента. Основное внимание уделено формированию цифровой культуры участников образовательного процесса, профилактике интернет-угроз и разработке системы педагогических мер по обеспечению безопасного цифрового пространства в школах. Монография адресована преподавателям, исследователям, методистам и всем, кто заинтересован в инновационных подходах к обучению. Монография выполнена в рамках грантового проекта ИРН AP19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента».

ISBN 978-601-267-831-4

**Оглавление**

# Введение

В условиях стремительной цифровизации общества и образования вопрос обеспечения кибербезопасности в школьной среде становится одной из ключевых задач современной педагогики. Цифровая трансформация охватывает все аспекты школьной жизни: от электронных журналов до онлайн-обучения и облачных хранилищ персональных данных. Вместе с новыми возможностями появляются и новые угрозы — кибербуллинг, фишинг, утечки персональных данных, деструктивный контент. В связи с этим перед образовательными учреждениями остро стоит задача выстраивания целостной системы защиты цифровой среды, ориентированной не только на технические, но и на педагогические решения.

Анализ современных исследований показал, что недостаточная цифровая грамотность участников образовательного процесса, слабое осознание рисков и отсутствие системной профилактической работы ведут к увеличению числа киберинцидентов. Вместе с тем, ключевую роль в формировании безопасной школьной среды играет педагог — носитель не только знаний, но и культуры цифрового поведения. Поэтому становится необходимым научно обоснованное внедрение педагогических механизмов, направленных на формирование у обучающихся и педагогов устойчивых навыков кибербезопасного поведения.

Одним из действенных инструментов такой системной работы выступает комплаенс-менеджмент — подход, заимствованный из сферы корпоративной этики и адаптированный к образовательной среде. Комплаенс ориентирован на соблюдение нормативных и этических стандартов, что позволяет выстраивать поведенческие рамки и регламенты цифровой безопасности, согласованные со всеми участниками процесса: администрацией, учителями, родителями и учениками.

Целью настоящей монографии является теоретическое обоснование и практическая реализация модели педагогического обеспечения кибербезопасности школьной среды на основе принципов комплаенс-менеджмента. В ходе исследования была проведена систематизация научных подходов, проанализированы нормативные документы, а также разработаны и апробированы методические материалы и цифровые ресурсы.

Основная научная проблема исследования заключается в отсутствии комплексной модели педагогического сопровождения цифровой безопасности школьной среды с опорой на комплаенс-инструменты. Монография направлена на восполнение этого дефицита и предлагает научно обоснованные рекомендации для педагогов, администраций школ и других заинтересованных сторон.

# 1 ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПЕДАГОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

## 1.1 Кибербезопасность как компонент цифровой грамотности

Современная образовательная система функционирует в условиях стремительного развития цифровых технологий и глобального распространения информационно-коммуникационных средств. Это создает не только новые возможности для обучения, но и порождает целый спектр рисков и угроз, особенно в контексте безопасности обучающихся в цифровом пространстве. На этом фоне особое значение приобретает формирование цифровой грамотности, одним из ключевых компонентов которой является кибербезопасность.

Проблема заключается в том, что традиционное понимание цифровой грамотности долгое время сводилось исключительно к техническим навыкам владения устройствами и программами. Однако в условиях цифровой среды, насыщенной киберугрозами, этого недостаточно. Современное образование требует переосмысления подходов к обучению и подготовки педагогов, способных не только использовать цифровые технологии, но и обучать безопасному и ответственному поведению в сети.

Актуальность темы усиливается тем, что учащиеся все чаще становятся жертвами киберзапугивания, утечки персональных данных и других форм цифрового насилия. При этом уровень осведомлённости педагогов и родителей о механизмах защиты от подобных угроз остается фрагментарным. Это требует системной подготовки и повышения квалификации всех участников образовательного процесса в области кибербезопасности как важнейшего аспекта цифровой грамотности.

Значимость данной проблемы заключается в необходимости выстраивания безопасной цифровой среды в школе как основы успешной социализации и развития учащихся. Кибербезопасность становится неотъемлемым условием полноценного включения в цифровую культуру XXI века, а цифровая грамотность — универсальной компетенцией, обеспечивающей не только технологическое, но и этическое, правовое и социальное ориентирование личности в цифровом мире.

Развитие информационного общества породило широкий спектр проблем, охвативших практически все сферы человеческой деятельности. Трансформации, обусловленные повсеместным распространением информационно-коммуникационных технологий (ИКТ), в значительной степени затронули и сферу образования. В

последние годы активно ведутся дискуссии, посвящённые характеру изменений, вызваных цифровыми медиа. В рамках этих обсуждений было представлено множество положительных оценок и научных исследований, подтверждающих эффективность применения ИКТ в образовательной практике. Проведённый анализ выявил и потенциальные угрозы, связанные с новыми медиа.

Очевидно, что как продуктивное использование ИКТ, так и предупреждение их возможных негативных последствий требуют достаточного уровня цифровой грамотности. С учётом стремительности происходящих изменений, способность ориентироваться в медиа-пространстве, понимание задействованных процессов, а также осознание взаимосвязей между человеком и информационными технологиями становятся необходимостью и требуют постоянного обновления знаний и навыков. Формирование цифровой грамотности в образовательном процессе должно учитывать не только её позитивный потенциал, но и возможные риски, сопряжёные с использованием цифровых медиа.

В контексте обеспечения цифровой безопасности цифровая грамотность всё чаще рассматривается с позиции праксилогического подхода [1]. Это связано с тем, что школьные учителя проводят профилактические мероприятия, направленные на минимизацию рискованного поведения, связанного с использованием цифровых медиа. Чаще всего это касается:

- киберзапугивания учащихся [2];
- киберзапугивания учителей [3];
- проблем использования интернет-технологий [4];
- понимания механизмов онлайн-злоупотреблений [5];
- защиты имиджа [6].
- нарушений законодательства об интеллектуальной собственности [7] и многих других электронных угроз.

Все эти проблемы находятся в состоянии постоянной эволюции, сопровождаясь как изменением масштабов существующих угроз, так и появлением новых форм рискованного поведения [8], [9]. Согласно данным исследования EU KIDS, молодёжь активно использует цифровые медиа, однако при этом испытывает потребность в сопровождении и поддержке. Особое значение при этом приобретает развитие их цифровой грамотности, в частности в аспекте обеспечения безопасности в онлайн-среде [10].

Защита от угроз школьников — это обязанность значимых людей, таких как родители и учителя. Учитывая сложность проблемных ситуаций, связанных с использованием информационно-коммуникационных технологий (ИКТ), взрослые должны обладать навыками, которые выходят за рамки обычного использования новых медиа в информационных и развлекательных целях. Эти навыки

необходимы для содействия адекватной социализации в средствах массовой информации [11].

Обеспечение безопасной цифровой среды возможно, в частности, за счёт интеграции разнообразных форм, методов и дидактических подходов, включённых как в формальные, так и в неформальные образовательные программы с ранних этапов обучения. Это обусловлено широким проникновением цифровых медиа в школьную, семейную и общественую сферы [12]. В условиях стремительного развития технологий цифровая грамотность приобретает статус одной из ключевых компетенций XXI века. Особенно актуально это в свете тех оброзовательных вызовов, с которыми сегодня сталкиваются педагоги и родители, — вызовов, значительно отличающихся от проблем, характерных для аналоговой эпохи [13].

Педагоги и родители должны не только действовать проактивно в вопросах предотвращения цифровых угроз, но и обладать актуальными знаниями о современных формах цифровых и гибридных рисков [14]. Следует отметить, что уровень осведомлённости учителей в области цифровых медиа во многом определяется их личным отношением к цифровым устройствам, таким как Интернет, компьютеры, планшеты и мобильные телефоны. Негативное восприятие этих технологий может существенно ограничивать понимание как их положительных, так и отрицательных сторон.

Воздействие информационно-коммуникационных технологий (ИКТ) на поведение детей и подростков, а также на условия образовательного процесса, подробно рассматривается в ряде научных исследований [15]. Анализ отношения и компетенций учителей и будущих педагогов в области ИКТ демонстрирует, что данная профессиональная группа характеризуется высокой степенью неоднородности с точки зрения цифровой грамотности и уровня технологической адаптации.

О неоднородности свидетельствует, например, умение педагогов свободно ориентироваться на веб-сайтах, пользоваться оборудованием и электронными сервисами, а также различное отношение к использованию новых медиа в образовании [16], [17]. В связи с этим при оценке уровня цифровой грамотности (Digital Literacy, DL) необходимо учитывать разнообразие знаний, умений и установок педагогов, независимо от их профессионального уровня или страны проживания. Эксперты подчёркивают важность специализированных неформальных образовательных программ, ориентированных на развитие как технических, так и социальных аспектов цифровой грамотности. Такие инициативы рассматриваются как эффективный способ повышения DL и коррекции отношения к цифровым медиа [18].

Учитывая широкий спектр киберугроз, затрагивающих не только

взрослых — включая педагогов и родителей — но в первую очередь детей и подростков, особая роль в профилактике и реагировании на цифровые инциденты в образовательной среде отводится именно учителям. Они несут ответственность за своевременное выявление проблемных ситуаций и развитие у обучающихся соответствующих навыков и компетенций. Отдельные старшеклассники, обладая более высоким уровнем цифровых навыков, демонстрируют способность к самостоятельной защите от цифровых угроз, что подчёркивает необходимость соответствующего уровня цифровой компетентности среди учащихся [19]. Вместе с тем, действующая система академической подготовки педагогов, включающая краткосрочные курсы продолжительностью 10–12 часов по направлениям медиапедагогики, цифровых технологий в образовании и ИКТ, остаётся недостаточной для полноценного формирования необходимых знаний и навыков. На практике педагоги расширяют свою цифровую компетентность преимущественно через решение реальных задач в образовательной среде, взаимодействие с коллегами, участие в целевых курсах повышения квалификации, а также посредством самообразования [20].

В условиях стремительного развития цифрового общества понятие цифровой грамотности продолжает трансформироваться. Эти изменения обусловлены как ростом IT-сектора, так и усложнением угроз, связанных с использованием цифровых технологий. В контексте школьного образования цифровая грамотность педагогов трактуется как способность эффективно применять цифровые устройства, онлайн-сервисы и веб-ресурсы в образовательной практике [21]. Особое значение при этом приобретает педагогическая функция цифровых медиа, особенно в аспекте повышения эффективности учебного процесса и интеграции мультимедийных элементов в дидактику [22].

Содержательно цифровая грамотность охватывает как технические, так и социальные компоненты. Технический аспект предполагает владение инструментами цифрового обучения, такими как интерактивные доски, компьютеры, планшеты и смартфоны, которые используются в качестве дидактических ресурсов [23]. Однако, наряду с техническими умениями, ключевую роль играют социальные аспекты цифровой грамотности [24], включая осознание рисков, связанных с цифровыми угрозами, и навыки безопасного поведения в цифровом пространстве.

Таким образом, цифровая грамотность представляет собой комплексное явление, объединяющее знание и умение свободно использовать цифровые медиа, а также понимание угроз, присущих цифровой среде. В частности, «мягкие» аспекты цифровая грамотность включают навыки предотвращения электронных рисков, понимание социально-психологических механизмов взаимодействия в

интернете, а также способность критически осмысливать как позитивные, так и негативные последствия цифровых технологий. Эти элементы столь же важны для успешной навигации в цифровом мире, как и умения работать с техническими средствами и программными ресурсами.

Существенным компонентом цифровой грамотности является критическая оценка контента, распространяемого в интернете [25]. Умение проверять достоверность информации в цифровой среде приобретает такое же значение, как и способность оценивать данные, поступающие из традиционных медиа. Это подчёркивает, что цифровая грамотность охватывает компетенции, актуальные как для онлайн-, так и для офлайн-реальностей [26].

Следовательно, рисковое поведение при взаимодействии с медиа следует анализировать не только с позиции технической оснащённости индивида, но и с учётом его когнитивных и поведенческих установок, влияющих на интерпретацию и использование цифрового контента. К сожалению, в существующей литературе анализ цифровой грамотности часто ограничивается самооценкой технических навыков работы с цифровыми устройствами и электронными ресурсами, в то время как компонент цифровой безопасности остаётся недооценённым.

Это свидетельствует о необходимости пересмотра подходов к определению структуры цифровой грамотности. Важной задачей становится разработка комплексных инструментов для измерения и сопоставления всех её составляющих. В современных реалиях цифровая безопасность становится не менее значимой, чем любые аспекты, касающиеся профилактики традиционных офлайн-угроз. За последние годы отмечается существенный рост количества публикаций и научных исследований, посвящённых вопросам информационной и электронной безопасности [27]. Было даже заявлено, что электронные угрозы стали основой для нового направления исследований в медиапедагогике, которое получило название "парадигма риска" (в отличие от "парадигмы возможностей").

Обеспечение цифровой безопасности, независимо от возраста, требует определённого уровня цифровой грамотности [28]. Базовые знания и навыки, связанные с минимизацией электронных угроз в области защиты конфиденциальных данных, пониманием механизмов киберзапугивания, проблемного использования Интернета и электронных азартных игр, становятся всё более важными в контексте цифровой грамотности [29]. Цифровая грамотность не только предполагает свободное использование цифровых медиа, но и означает понимание того, как ИКТ влияют на поведение пользователей в Интернете и способствуют рискованному поведению [30].

Особую роль в минимизации негативных последствий, связанных с насыщением новыми технологиями, играют ближайшее окружение индивидов, включая родителей и других значимых людей, особенно учителей в образовательных учреждениях [31]. Учителя должны обладать современными знаниями об угрозах, которые несёт цифровой мир, и быть способны моделировать DL в этой области, например, с помощью комплексных профилактических программ [32]. Сегодня учителя несут ответственность не только за предотвращение офлайн- и онлайн-угроз, но и за гибридные угрозы, которые пересекают границу между этими двумя формами [33].

Отношение учителей к цифровой грамотности варьируется в зависимости от различных факторов, представленных в эмпирической части исследования. Поэтому обсуждение компонентов цифровой грамотности и программ поддержки, таких как неформальное образование учителей, становится одной из задач медиаобразования. Учителя сталкиваются с различными формами рискованного поведения, опосредованного Интернетом, в процессе социализации и медиаобразования [34].

Рассмотренные исследования показывают, что уровень риска среди респондентов неоднороден. Преподаватели демонстрируют относительно высокий уровень знаний и навыков в области эргономики использования новых технологий, что особенно важно для формирования позитивных привычек у учащихся на втором этапе обучения. Наиболее слабым компонентом цифровой грамотности является авторское право [35]. Примеры низкой осведомлённости о проблемах, связанных с авторским правом, включают использование материалов, загруженных из Интернета (видео, музыка, программное обеспечение), на уроках, что не всегда соответствует законодательству об авторском праве.

Из-за масштабов рискованного поведения и постоянного появления новых областей риска концепция цифровой грамотности (DL) является изменчивой и требует постоянного пересмотра [36].

Анализ исследований, приведенных выше, показал, что существует группа учителей, которые добились более высоких результатов в тестах благодаря своему отношению к новым медиа. Таким образом, технооптимисты гораздо более информированы, чем технопессимисты [37]. Учителя, которые регулярно используют ИКТ в своей работе, пользуются электронными учебниками или считают, что новые медиа способствуют большей вовлеченности их учеников, получили статистически более высокие результаты. Таким образом, отношение, знания и грамотность, связанные с цифровыми медиа, часто связаны с типом знаний о негативных последствиях насыщения школ и жизни учащихся ИКТ [38], [39].

Интересен также аспект оценки респондентами своего уровня грамотности. Чаще всего учителя оценивают свою грамотность как

среднюю или высокую.

DL — это многогранная конструкция, которая включает в себя техническую возможность использования устройств и веб-сайтов, просмотр информации, защиту данных, настройку оборудования и обновление знаний о новых электронных угрозах. Все эти факторы затрудняют перечисление и измерение всех показателей цифровой безопасности. Однако мы заметили, что чем выше осведомленность и грамотность в одной области, тем выше уровень знаний в других областях.

Представленные результаты вписываются в дискуссию о функционировании школ в эпоху цифровых технологий. Современная школа — это учреждение, которое не только внедряет информационные технологии и управленческие решения в свою образовательную практику, но и готовит учащихся к успешной защите от растущего числа электронных угроз [40].

Ключевым элементом в процессе укрепления цифровой грамотности (DL) среди учащихся является компетентный, целенаправленно действующий преподаватель [41], [42]. Это предположение требует более широкого обсуждения изменений в информационном обществе и связанных с ними как положительных, так и отрицательных последствий. Концепция обучения на протяжении всей жизни, поддерживаемая профессиональным сектором (НПО, неформальным образованием и самообразованием учителей), становится ответом на необходимость обновления или расширения DL по мере возникновения новых обстоятельств. Однажды приобретённые знания о цифровых угрозах представляют собой набор информации, который необходимо постоянно расширять и обновлять [43]. С этой точки зрения концепция цифровой грамотности становится интегрирующей конструкцией, подверженной постоянным преобразованиям.

Таким образом, кибербезопасность неразрывно связана с понятием цифровой грамотности и должна рассматриваться как её базовый компонент, требующий системного внедрения в образовательную практику. Образовательные учреждения обязаны не только осваивать новые цифровые инструменты, но и формировать культуру безопасного поведения в информационной среде, начиная с раннего возраста.

Проведённый анализ показывает, что эффективная цифровая социализация невозможна без участия компетентного педагога, обладающего актуальными знаниями о киберугрозах, навыками их предотвращения и готовностью к постоянному обновлению цифровой компетентности. Это требует как пересмотра содержания подготовки педагогов, так и создания комплексных профилактических программ, ориентированных на защиту всех участников образовательного процесса.

В условиях постоянной трансформации цифровой среды понятие цифровой грамотности становится подвижной и интегрирующей конструкцией, объединяющей технические и социальные компоненты. Современный подход к DL должен охватывать не только использование цифровых средств, но и критическое мышление, этическое поведение и правовую грамотность в цифровом пространстве.

Следовательно, устойчивое развитие цифровой грамотности невозможно без глубокого понимания и активного включения аспектов кибербезопасности. Это важнейшая задача как для образовательной политики, так и для научных исследований, направленных на формирование безопасной и ответственной цифровой культуры.

## 1.2 Дескрипторы базовых понятий кибербезопасности в свете современного состояния проблемы и системообразующих признаков безопасной образовательной среды

В современных условиях цифровой трансформации образования вопросы кибербезопасности приобретают особое значение для Казахстана. Быстрое внедрение электронных журналов, дистанционного обучения, облачных платформ и многоязычных образовательных ресурсов сопровождается необходимостью обеспечить надежную защиту информации и устойчивость образовательного процесса. В этой связи ключевое значение имеют базовые дескрипторы кибербезопасности, которые выполняют функцию понятийных ориентиров и практических регуляторов при формировании безопасной образовательной среды. Они отражают как технические, так и организационно-педагогические аспекты, определяя системность и целостность подхода к информационной защите в образовательных учреждениях.

Прежде всего, важным является принцип конфиденциальности, обеспечивающий сохранность персональных данных обучающихся и педагогов. Для Казахстана эта проблема особенно актуальна в связи с тем, что государство активно развивает цифровые сервисы «Электронной школы» и платформы для мониторинга образовательных достижений, аккумулирующие большие объемы информации. Нарушение конфиденциальности в таких системах не только угрожает частной жизни граждан, но и подрывает доверие к образовательным институтам. Важной задачей становится создание политики управления доступом, внедрение механизмов шифрования и контроль за использованием учетных записей.

Не менее значимым дескриптором является целостность данных, под которой понимается их неизменность и корректность.

Нарушение этого принципа в образовательной среде может привести к подделке оценок, искажению учебных планов или манипуляциям с результатами экзаменов. В условиях Казахстана, где растет роль централизованных баз данных и единой образовательной информационной системы, вопрос целостности приобретает стратегическое значение. Его обеспечение возможно через регулярное резервное копирование, контроль версий данных и ведение журналов изменений [44].

Принцип доступности также является краеугольным камнем безопасной образовательной среды. В период пандемии COVID-19 Казахстан, как и многие другие страны, столкнулся с проблемой перегрузки серверов и перебоев в работе платформ дистанционного обучения. Эти ситуации наглядно показали, что без разработки планов обеспечения непрерывности деятельности и внедрения отказоустойчивых решений образовательный процесс оказывается под угрозой. Доступность цифровых ресурсов напрямую связана с обеспечением равного права на образование, а значит, выступает не только техническим, но и социальным фактором.

Два связанных дескриптора – аутентификация и авторизация – формируют систему управления доступом в образовательных организациях. Их правильная реализация особенно важна для многоязычных школ и университетов Казахстана, которые используют различные электронные платформы для обучения на разных языках и взаимодействия с международными партнерами. Ошибки в этих процессах могут привести к компрометации учетных записей и избыточным полномочиям пользователей. Применение принципа минимальных прав, многофакторной аутентификации и централизованного управления доступом позволяет существенно снизить эти риски.

Мониторинг и контроль цифровых систем необходимы для своевременного выявления аномалий и угроз. В условиях Казахстана, где в последние годы фиксируются атаки на государственные и образовательные ресурсы, именно регулярный аудит и использование систем обнаружения вторжений становятся основой устойчивости. Прозрачность и отслеживаемость действий пользователей усиливаются введением обязательных журналов активности и логирования.

Однако обеспечение кибербезопасности невозможно без формирования соответствующей культуры среди участников образовательного процесса. Дескриптор обучения и повышения осведомленности пользователей особенно важен в казахстанских школах и университетах, где цифровая грамотность педагогов и студентов все еще развивается неравномерно. Недостаточные знания в области безопасности способствуют распространению фишинга, социальной инженерии и других угроз. В этой связи регулярные

тренинги, практические занятия и интеграция вопросов цифровой безопасности в учебные программы являются неотъемлемой частью формирования устойчивой образовательной среды [45].

С этим тесно связано понятие ответственности, которая выражается в прозрачности действий и подотчетности каждого участника образовательного процесса. В казахстанской практике наблюдается потребность в четком распределении обязанностей между администрацией школ, учителями и техническими специалистами, что позволит повысить уровень доверия и минимизировать риски.

Наконец, принцип непрерывности процессов отражает способность образовательных организаций функционировать даже в условиях инцидентов. Для Казахстана актуальным становится создание планов аварийного восстановления, развитие дублирующей инфраструктуры и резервных каналов связи, особенно в сельских школах, где цифровые ресурсы зачастую ограничены.

Ниже представлена графическая схема девяти базовых понятий кибербезопасности в образовательном контексте (рисунок 1.2.1).

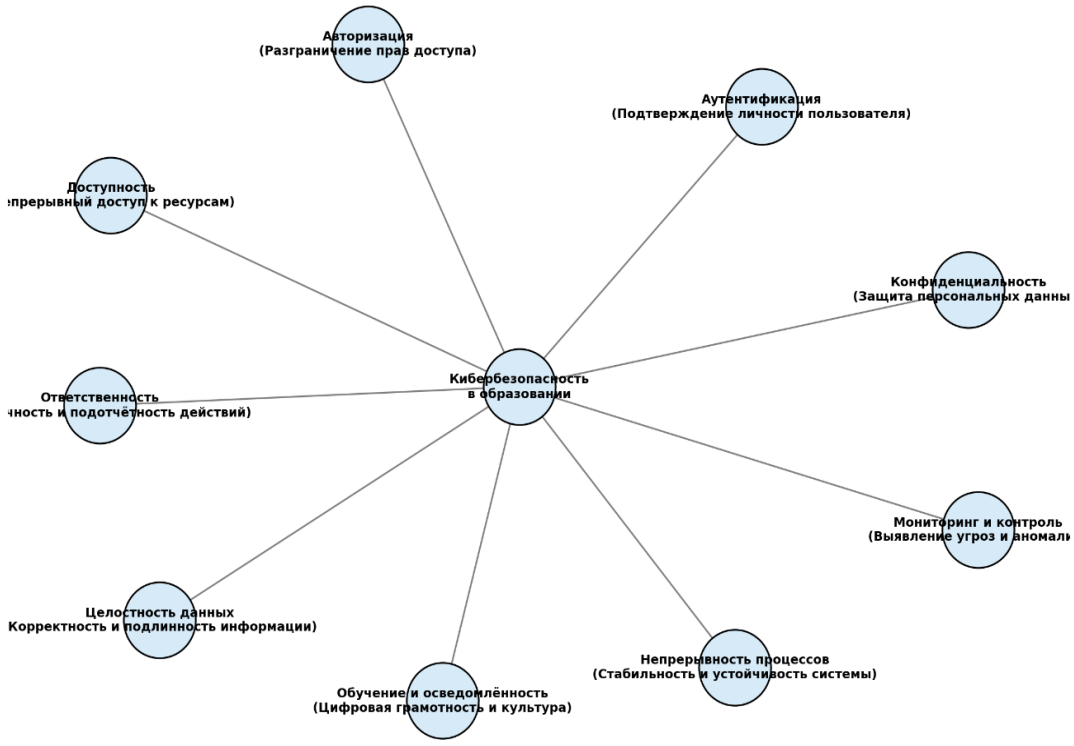



Рисунок 1.2.1 – Дескрипторы кибербезопасности в образовательной среде (с пояснениями)

Помимо указанных выше базовых понятий в практике обеспечения кибербезопасности применяются и другие понятия. Мы посчитали целесообразным расширить данный перечень, так как в

современном обществе, характеризующемся стремительным развитием информационных технологий и массовой цифровизацией всех сфер жизненной деятельности, кибербезопасность вступает одной из ключевых категорий, определяющих устойчивость как отдельных информационных систем, так и государства в целом. Под данным понятием понимается комплекс мер и стратегий, направленных на защиту данных, компьютерных устройств, сетей и пользователей от внешних и внутренних угроз, включая кибератаки, несанкционированный доступ и различные формы злоумышленный активности. Важна подчеркнуть, что кибербезопасность имеет между дисциплинарный характер: она объединяет технические средства защиты, правовое регулирование, организационные меры, а также психологические аспекты взаимодействия пользователей с информационной среды.

Среди базовых категорий кибербезопасности особое значение занимает понятие угрозы информационной безопасности [46, 47, 48]. Угроза представляет собой потенциальную возможность возникновения событий или действий, способных нанести ущерб данным, системам или пользователям. Угрозы могут иметь как технологическую, так и человеческую природу? От вирусных атак и фишинговых писем до ошибок сотрудников или халатности в соблюдении регламентов безопасности. Характер угроз во многом определяется наличием уязвимостей – слабых мест в программном обеспечении, аппаратных средствах или человеческом факторе. Классическим примером уязвимости выступает использование слабых паролей, установка устаревших программных версий или игнорирование обновлений безопасности [49].

Именно сочетание угроз и уязвимостей открывает возможность для кибератак – целенаправленных действий злоумышленников, направленных на подрыв работоспособности систем, кражу информации или нанесение ущерба пользователям и организациям. Кибератаки имеют многообразные формы: от традиционных вирусных заражений и сетевых проникновений до масштабных атак отказа в обслуживании (DDoS), которые парализуют деятельность интернет-ресурсов посредством искусственной перегрузки запросами. Эти процессы наглядно демонстрируют необходимость комплексного подхода к обеспечению безопасности в цифровой среде.

Фундаментальной основой теоретического понимания кибербезопасности служит так называемая CIA-триада (Confidentiality – Integrity – Accessibility), включающая три взаимосвязанных принципа: конфиденциальность, целостность и доступность данных [50]. Конфиденциальность означает сохранение данных в неизменном виде, исключая возможность их искажения; доступность указывает на необходимость обеспечения легитимным пользователям возможности использовать данные и системы в нужный момент. Так, онлайн-

банкинг должен одновременно гарантировать защиту персональных данных клиента, исключать возможность несанкционированных изменений в базе и обеспечивать круглосуточный доступ к сервису.

Ключевыми процессами в практической реализации безопасности вступают аутентификация и авторизация. Первое представляет собой процедуру проверки личности пользователя, реализуемую через ввод пароля, биометрические данные или многофакторную схему защиты. Авторизация же обеспечивает разграничение прав пользователей после успешной аутентификации, позволяя определять уровень их доступа к ресурсам. Данная пара категорий иллюстрирует принцип «минимальных привилегий», когда каждый пользователь получает только тот уровень доступа, который необходим для выполнения его функций [51].

Немаловажное место в системе кибербезопасности занимает шифрование, представляющие собой преобразование данных в закодированный вид, доступный для понимания лишь обладателям соответствующих ключей. Современные системы принимают как симметричные алгоритмы, основанные на едином ключе, так и асимметричные методы с использованием пары ключей- открытого и закрытого. Шифрование широко применяется как при передаче данных по сетям связи, так и при их хранении на устройствах или в облачных сервисах [52, 53].

В практической плоскости особое внимание уделяется вопросам парольной безопасности. Пароль продолжает оставаться наиболее распространенным методом защиты, однако его эффективность на прямую зависит от сложности и грамотности использования. Слабые или стандартные пароли (например, «123456» или «qwerty») многократно повышают риск компрометации. Поэтому современные рекомендации включают использование длинных, уникальных комбинаций, включающих буквы разных регистров, цифры и специальные символы, а также хранение паролей в специализированных менеджерах.

Отдельный пласт угроз составляют вредоносные программы (malware), создаваемые с целью нанесения ущерба пользователя или получения неправомерного доступа к данным. К данному классу относятся вирусы, троянские программы, сетевые черви, шпионская ПО, кейлоггеры, а также вымогатели (ransomware), шифрующие файлы и требующие выкуп. Подобные угрозы могут распространяться через официальные магазины приложений.

На пересечении психологических и технических факторов находится явление фишинга и более широкое понятие социальной инженерии. Фишинг представляет собой метод обмана пользователей посредством поддельных сайтов или сообщений, имитирующих доверенные источники (банки, социальные сети государственные порталы). Социальная инженерия, в свою очередь, охватывает весь

спектр манипуляций человеческим поведением с целью получения доступа к конфиденциальной информации: от телефонных звонков «сотрудников банка» до инсценированных просьб коллег. Эти методы демонстрируют, что слабым звеном в системе безопасности нередко является сам человек.

Особое внимание в контексте защиты информационных систем уделяется средствам предотвращения атак [50]. Среди них важнейшими являются брандмауэры (firewalls), выполняющие функцию фильтрации сетевого трафика и блокировки подозрительных подключений, а также антивирусные программные обеспечение, которая анализирует файлы и процессы, выявляет вредоносные объекты и препятствует их запуску. Неотъемлемым элементом современной цифровой безопасности является использование VPN (Virtual Private Networking), обеспечивающего защищенный канал передачи данных и позволяющего скрывать активность пользователя в сети.

Не менее значимой является практика резервного копирования (бэкапа). Данный процесс предусматривает регулярная создание копий данных, что позволяет восстановить их в случае утраты, повреждения или кибератаки. В профессиональной среде распространено правило «3-2-1»: три копии данных, две на разных носителях, одна в Облаке. Таким образом обеспечивается устойчивость к любым инцидентам, включая физическое повреждение оборудование.

Наконец, система образующим элементом обеспечения кибербезопасности вступает политика информационной безопасности – совокупность правил и регламентов, определяющих порядок работы с информацией в организации. Она охватывает как технические аспекты (парольная политика, использование корпоративных устройств), так и организационные меры (распределение ответственности, обучение сотрудников). Именно наличие продуманный политики позволяет систематизировать меры защиты и минимизировать человеческий фактор, который, по статистике, является причиной значительной части инцидентов [54].

Таким образом, базовые понятия кибербезопасности образуют целостную систему, в которой каждое звено связано с другими [55, 56]. Угрозы и уязвимости формируют почву для атак, противостоять которым позволяют технические средства защиты, организационные регламенты и образовательные практики. Концептуальная триада «конфиденциальность – целостность – доступность» задает основу для построения комплексных стратегий защиты, а инструменты, такие как шифрование, аутентификация, резервное копирование и использование VPN служат практическими механизмами их реализации. При этом ключевым условием успешного функционирования систем безопасности остается гармоничное

сочетание технологий и человеческого Фактора, что требуют не только внедрение средств защиты, но и постоянного повышения цифровой грамотности пользователей.

Таблица «Базовые понятия кибербезопасности»

| № | Термин | Определение | Пример |
|---|---|---|---|
| 1 | Кибербезопасность | Защита данных, устройств и сетей от атак и несанкционированного доступа | Использование антивируса и VPN на компьютере |
| 2 | Угроза информационной безопасности | Потенциальное событие, которое может повредить системе или данным | Письмо с подозрительным вложением |
| 3 | Уязвимость | Слабое место, которое может использовать злоумышленник | Пароль «123456» или устаревшее ПО |
| 4 | Кибератака | Намеренные действия хакеров для получения доступа или нанесения ущерба | Массовая рассылка вирусов |
| 5 | CIA-триада | Принципы: конфиденциальность, целостность, доступность данных | Онлайн-банк: защита данных, отсутствие изменений посторонними, работа 24/7 |
| 6 | Аутентификация | Проверка личности пользователя | Вход в соцсети по паролю или отпечатку пальца |
| 7 | Авторизация | Предоставление прав доступа после входа | Ученик может читать дневник, учитель – редактировать |
| 8 | Шифрование | Кодирование данных для защиты от посторонних | Переписка в WhatsApp защищена сквозным шифрованием |
| 9 | Парольная безопасность | Использование устойчивых и сложных паролей | Пароль «MyDog2024!», а не «qwerty» |
| 10 | Вредоносное ПО (Malware) | Программы для нанесения вреда или кражи информации | Рансомварь шифрует файлы и требует деньги |
| 11 | Фишинг | Обман с целью получения личных данных | Письмо «Ваша карта заблокирована, введите пароль» |
| 12 | Социальная инженерия | Манипуляция людьми ради получения доступа | Звонок от «сотрудника банка» с просьбой сообщить код |
| 13 | DDoS-атака | Перегрузка сайта множеством запросов | Онлайн-магазин перестал работать в «Черную пятницу» |
| 14 | Брандмауэр | Фильтрация сетевого | Firewall блокирует |

| | | | |
|---|---|---|---|
| | (Firewall) | трафика для защиты системы | попытку удаленного взлома |
| 15 | Антивирус | Программа для обнаружения и удаления вредоносного ПО | Avast предупреждает о зараженном файле |
| 16 | VPN | Защищенное интернет-соединение | Студент использует VPN для безопасного доступа к университетской сети |
| 17 | Бэкап | Резервное копирование данных для восстановления | Фото автоматически сохраняются в облако |
| 18 | Политика информационной безопасности | Правила защиты данных организации | Запрет на использование личных флешек в школе |

Таким образом, приведенные дескрипторы – конфиденциальность, целостность, доступность, аутентификация, авторизация, мониторинг, обучение, ответственность и непрерывность и другие – в совокупности формируют основу кибербезопасности в казахстанской образовательной среде. Их комплексная реализация позволяет не только минимизировать риски кибератак, но и создать условия для устойчивого функционирования системы образования, способной эффективно решать задачи цифровизации и многоязычного развития в условиях глобальных вызовов.

## 1.3 Характеристика факторов негативного психоманипулятивного воздействия киберугроз

В начале XXI века в социальной реальности происходят существенные изменения, связанные с активным проникновением новых информационных технологий в общественные процессы. Появление новой компьютеризированной техники, в том числе смартфонов и гаджетов, оснащенных выходом в Интернет, способствовало изменению отношения к информации, способам взаимодействия, что отразилось на всех социальных, экономических, политических и даже культурных процессах, то есть изменился образ жизни человека в новом обществе.

Вопросы влияния активного использования гаджетов с выходом в Интернет на здоровье пользователей обсуждаются в мире с конца XX века. Выявлено влияние неправильного использования гаджетов и неконтролируемого доступа в Интернет на физическое [57, 58], психическое [59, 60], духовное [61] и социальное [62, 63] здоровье подрастающего поколения. Эти эффекты можно в совокупности назвать киберугрозами в детском и подростковом возрасте.

Киберугрозы представляют собой серьезную опасность для индивидуумов в школьной среде. Одним из наиболее тревожных

аспектов киберугроз является их способность к психоманипуляции, что может привести к негативным последствиям для психического здоровья и благополучия пользователей.

В школьной среде существует множество киберугроз, с которыми сталкиваются как ученики, так и учителя. Эти угрозы включают в себя фишинг, вредоносное программное обеспечение, кибербуллинг, утечку личных данных, шантаж и вымогательство. Важно понимать, что кибербезопасность в школе – это не только защита от вирусов, но и комплексный подход к обучению правильному поведению в интернете.

Современные школьники осваивают цифровое пространство раньше, чем умеют читать. Они начинают взаимодействовать с различными гаджетами и интернет-платформами с раннего возраста, что открывает множество возможностей для обучения, общения и развлечений. Однако, чем активнее подростки выходят в онлайн-среду, тем выше риск стать жертвами киберзависимости и психоманипулятивного воздействия.

Киберзависимость — это состояние, при котором человек не может противостоять Интернету, социальным сетям, видеоиграм или другим цифровым платформам, что негативно сказывается на его повседневной жизни, учебе и социальных отношениях. Дети и подростки, проводящие много времени в сети, могут столкнуться с различными проблемами, такими как снижение успеваемости в школе, ухудшение межличностных отношений и даже физические проблемы, связанные с малоподвижным образом жизни.

Кроме того, психоманипулятивное воздействие может привести к еще более серьезным последствиям, включая развитие тревожности, депрессии и других психических заболеваний. Подростки, погруженные в виртуальный мир, могут потерять способность адекватно воспринимать реальность, что делает их уязвимыми для манипуляций со стороны других пользователей, а также для различных киберугроз, таких как кибербуллинг, мошенничество и эксплуатация.

Стоит отметить, что киберзависимость, как негативное психоманипулятивное воздействие, — не единственное негативное последствие активного использования цифровых технологий. Наряду с ней возникают и другие риски, такие как потеря конфиденциальности, кража персональных данных, воздействие на психику через негативный контент. Поэтому особое внимание следует уделять формированию критического мышления, навыков безопасного поведения в Интернете, осознанию потенциальных опасностей у детей и подростков, чтобы они могли эффективно защитить себя в цифровом пространстве. В настоящее время социально-психологические исследования кибербезопасности сосредоточены в первую очередь на экстраполяции общих

закономерностей, наблюдаемых в традиционных формах взаимодействия, на сферу цифровой коммуникации и онлайн-активности. Это означает, что исследователи пытаются перенести давно устоявшиеся принципы и теории о поведении человека в офлайн-средах в контекст онлайн-взаимодействий.

Однако такие экстраполяции не всегда могут учитывать уникальные особенности цифровой среды, включая анонимность, географическую удаленность пользователей и динамизм взаимодействий. Например, пользователи могут вести себя более рискованно в онлайн-пространствах, чем в реальной жизни, возможно, из-за отсутствия немедленных последствий для своих действий или чувства безопасности, обеспечиваемого экраном.

Также важно отметить, что кибербезопасность охватывает не только технические аспекты, но и социальные, культурные и психологические факторы. Например, восприятие риска, уровень доверия к цифровым платформам и готовность пользователей следовать рекомендациям по безопасности требуют более глубокого анализа с точки зрения социальной психологии.

Таким образом, для лучшего понимания вопросов кибербезопасности необходимо развивать исследования, учитывающие как общие закономерности человеческого поведения, так и конкретные аспекты цифровых взаимодействий. Это позволит нам разрабатывать более эффективные стратегии повышения уровня безопасности и формирования ответственного поведения школьных пользователей в сети.

Рассмотрим основные факторы негативного психоманипулятивного воздействия на школьных пользователей.

*1.Дезинформация и фейковые новости:*

Психологическое воздействие дезинформации может привести к изменению мнения и поведения. В современном мире фейковая информация и фейковые новости распространены, особенно среди школьников, которые активно используют Интернет и социальные сети для получения информации. Распространение ложной информации может вызвать у них чувство неуверенности и тревоги, что в свою очередь негативно влияет на их психоэмоциональное состояние. Распространение ложной информации может вызвать у школьных пользователей чувство неуверенности и тревоги.

Психологическое воздействие дезинформации может быть довольно серьезным. Зачастую молодые пользователи, подвергающиеся воздействию противоречивой или ложной информации, начинают сомневаться в своих знаниях и оценках, что приводит к внутреннему конфликту и снижению самооценки. Более того, такие новости могут формировать искаженное восприятие действительности и способствовать распространению стереотипов и предвзятых взглядов.

Кроме того, ложная информация может привести к изменению мнений и поведения школьников. Они начинают принимать решения, основанные на ложных предпосылках, что может негативно влиять на их отношения с окружающими, а также на их учебную деятельность и социальные связи.

В мире постоянного потока информации важно научить молодежь критически оценивать источники и проверять факты, чтобы минимизировать влияние ложной информации и защитить их психическое здоровье.

*2.Социальная инженерия:*

Использование манипулятивных техник для получения конфиденциальной информации. Примеры: фишинг, предлог доверительного общения. Эти методы могут вызвать у жертв чувство вины или страха.

Социальная инженерия — это набор методов манипуляции, используемых для получения конфиденциальной информации или доступа к защищенным ресурсам. В отличие от традиционных методов взлома, требующих технических навыков, социальная инженерия опирается на психологию и человеческие слабости. Злоумышленники могут использовать различные стратегии, чтобы обманом заставить детей раскрыть личную информацию, такую как пароли или номера кредитных карт.

Одним из наиболее распространенных методов социальной инженерии является фишинг. В этом случае мошенники отправляют электронные письма или сообщения, которые выглядят как законные запросы от известных организаций, таких как банки или социальные сети. Эти сообщения часто содержат ссылки на поддельные веб-сайты, где жертв можно обманом заставить ввести свои данные.

Другим примером является мошенничество с доверием, когда злоумышленник устанавливает отношения с жертвой, выдавая себя за кого-то, кого он знает или с кем знаком. Это может происходить с помощью телефонных звонков, текстовых сообщений или даже личных встреч. Злоумышленник может манипулировать эмоциями жертвы с помощью тактик, которые заставляют ее действовать против ее воли, таких как чувство вины или страха. Например, они могут утверждать, что жертва нарушила закон или находится в опасности, что побудит ее предоставить необходимую информацию.

Эти методы социальной инженерии могут иметь серьезные последствия для жертв. Не только финансовые потери, но и эмоциональные эффекты, такие как вина, стыд или страх, могут оставить глубокие шрамы. Жертвы могут сомневаться в своей способности распознавать обман, что в свою очередь может привести к снижению уверенности в себе и ухудшению психологического состояния. Важно повышать осведомленность об этих методах и обучать людей тому, как защитить себя от манипулятивных тактик.

*3.Кибербуллинг:*

Нападения в интернете, которые могут вызвать у жертв депрессию, тревожность и даже суицидальные мысли. Анонимность интернет-пространства усиливает манипулятивное воздействие.

Кибербуллинг — это форма травли и преследования, которая происходит в сети и имеет серьезные последствия для жертв. В отличие от традиционных форм травли, кибербуллинг может происходить в любое время и в любом месте, что делает его особенно опасным. Атаки могут принимать различные формы, включая отправку оскорбительных сообщений, распространение слухов, публикацию компрометирующих фотографий и даже создание фейковых аккаунтов для травли.

Кроме того, кибербуллинг может включать в себя постоянное преследование жертвы в социальных сетях, оставление негативных комментариев под постами травли или отправку угрожающих сообщений в личных сообщениях. Это создает атмосферу страха и тревоги, которая может значительно ухудшить психоэмоциональное состояние жертвы.

Стоит отметить, что кибербуллинг может затрагивать детей всех возрастов, но подростки и молодые люди чаще становятся его жертвами. Это связано с их активным использованием социальных сетей и других онлайн-платформ, что делает их уязвимыми для агрессии со стороны сверстников. Последствия кибербуллинга могут быть серьезными: жертвы часто испытывают депрессию, беспокойство, низкую самооценку, а в некоторых случаях даже мысли о самоубийстве.

Борьба с кибербуллингом требует комплексного подхода, включая обучение безопасному поведению в сети, поддержку жертв и осведомленность общественности о проблеме. Родителям, учителям и подросткам важно знать признаки кибербуллинга и то, как на него реагировать. Создание безопасной и поддерживающей онлайн-среды — это общая ответственность, которая требует усилий всех участников.

*4.Токсичная среда в социальных сетях:*

Постоянное сравнение себя с другими может вызвать низкую самооценку. Механизмы алгоритмов социальных сетей могут подталкивать к определенным эмоциям и реакциям.

В современном мире социальные сети стали неотъемлемой частью нашей жизни, но они также могут создавать токсичную среду, в которой пользователи испытывают негативные эмоции. Одним из самых распространенных явлений является постоянное сравнение себя с другими. Пользователи, просматривающие тщательно отобранные и отредактированные изображения и истории, часто начинают чувствовать, что их жизнь не соответствует идеалам, представленным в их новостных лентах. Это может привести к

снижению самооценки, чувству неполноценности и даже депрессии. Подростки и молодежь могут начать сомневаться в своих достижениях, внешности и способностях, что в свою очередь усиливает стресс и негативные эмоции.

Кроме того, механизмы алгоритмов социальных сетей играют важную роль в формировании эмоционального фона пользователей. Алгоритмы, направленные на удержание внимания, могут подталкивать пользователей к контенту, вызывающему сильные эмоции, такие как радость, гнев или страх. Это может привести к тому, что люди начнут воспринимать мир через призму крайних эмоций, что в свою очередь скажется на их восприятии самой жизни и их отношениях с окружающими. Например, постоянный поток негативных новостей или провокационный контент может вызывать чувства тревоги и беспокойства.

Таким образом, токсичная среда в социальных сетях не только влияет на самооценку пользователей, но и формирует их эмоциональное состояние, создавая порочный круг, из которого трудно вырваться. Важно знать об этих механизмах и стремиться к здоровому взаимодействию с социальными сетями, чтобы минимизировать их негативное влияние на психическое здоровье.

*5.Агрессивная реклама и таргетинг:*

Использование данных пользователей для создания манипулятивной рекламы может вызвать чувство зависимости или необходимости в определенных товарах и услугах.

Использование пользовательских данных для создания манипулятивной информации становится все более распространенной практикой в современном мире. Система образования собирает большие объемы информации о поведении, предпочтениях и привычках потребителей, чтобы максимально точно отображать свои информационные сообщения. Такой подход позволяет повышает эффективность информационных сообщений, но и поднимает серьезные этические вопросы.

Особенно опасен такой подход для уязвимых групп, таких как подростки с низкой информационной грамотностью, которые с большей вероятностью становятся жертвами навязчивого сообщения. Постоянное воздействие агрессивной информации может сформировать чувство зависимости или потребности в определенных направлениях, независимо от реальных возможностей. В результате у пользователя формируется иллюзия необходимости постоянного обновления информации.

Поэтому крайне важно регулировать такие практики, как повышение прозрачности данных и ограничение использования гипнотических технологий, чтобы поддерживать баланс между эффективностью информации и защитой прав потребителей.

*6.Психологическое давление со стороны киберугроз:*

Угрозы раскрытия личной информации (например, шантаж) могут вызвать сильный стресс и беспокойство. Угрозы раскрытия личной информации и психологическое давление со стороны киберугроз могут вызывать чувство тревоги и незащищенности у пользователей. Постепенное увеличение кибератак приводит к страху за свою безопасность и опасениям утечки данных, что может негативно сказаться на психоэмоциональном состоянии школьников. Помимо технических последствий, кибератаки наносят долгосрочные психологические раны учащимся и образовательным учреждениям. Жертвы часто ощущают подорванное доверие, напряжение и беспокойство

*7. Секретные манипуляции и шантаж:*

Использование личной информации для шантажа или манипуляции может быть сделано с целью получения денег или других ресурсов от жертвы. Такие действия часто осуществляются скрытно и тайно, что затрудняет их обнаружение и противодействие.

В большинстве случаев злоумышленники собирают и хранят компрометирующую информацию о жертве — например, личные фотографии, видео, переписку, информацию о ее финансовом положении или других уязвимых аспектах жизни. Затем они используют эти данные для оказания давления на человека, угрожая раскрытием этой информации или использованием ее против него.

Вымогательство может принимать форму требования немедленной оплаты, психологического давления, угрозы утечки персональных данных, клеветы или даже физического вреда. Такие методы нарушают основные принципы личной безопасности и конфиденциальности и требуют особого внимания со стороны правоохранительных органов и специалистов по кибербезопасности.

Важно помнить, что жертвам такого насилия следует обращаться за помощью, не поддаваться давлению и принимать меры по защите своих данных и прав.

*8. Подделка и имитация:*

Создание поддельных веб-сайтов, приложений или социальных сетей, это факт обмануть пользователя и получить доступ к его данным. Это также может привести к нарушению приватности и эмоциональному дискомфорту. Создание поддельных веб-сайтов, приложений или сайтов социальных сетей, чтобы обманом заставить пользователей предоставить свои данные.

Эти мошенничества часто выглядят очень похожими на настоящие, что затрудняет их идентификацию для ничего не подозревающих или неинформированных пользователей. Мошенники используют различные методы, такие как копирование дизайнов, логотипов и URL-адресов, чтобы обмануть пользователей, заставив их доверять им и вводить личные или финансовые данные. Это также может привести к серьезным нарушениям конфиденциальности и

краже личной информации, денег или коммерческой тайны. В результате пользователи могут испытывать эмоциональный стресс, чувство потери контроля над своей информацией и финансовые потери. Важность осознания этих угроз, а также использования двухфакторной аутентификации и надежного антивирусного программного обеспечения становится ключевым элементом защиты от этих типов мошенничества.

*9. Человеческий фактор:*

Дети могут стать жертвами манипуляций из-за недостатка знаний о киберугрозах или из-за своей доверчивости. Это может включать слабые пароли, отсутствие двухфакторной аутентификации и прочие уязвимости. Человеческий фактор: дети особенно уязвимы для киберугроз из-за отсутствия образования и высокой надежности. Это увеличивает риск стать жертвами мошенничества, фишинга и других видов атак. Отсутствие навыков может включать использование слабых паролей, неиспользование двухфакторной аутентификации, незнание того, как защищать личные данные и обрабатывать подозрительные сообщения или ссылки. Важно научить детей правилам безопасного поведения в сети и развивать критическое мышление в цифровой среде.

*10. Эмоциональное воздействие:*

Использование эмоциональных триггеров, таких как страх, чувство срочности или неуверенность, чтобы заставить пользователя действовать против его интересов или раскрыть личные данные. Эмоциональное воздействие: злоумышленники часто используют эмоциональные триггеры для манипулирования пользователями. Это сообщения, которые вызывают страх («ваша учетная запись заблокирована», «вы выиграли приз»), чувство срочности («вам нужно действовать быстро») или неуверенности. Такая тактика побуждает людей действовать быстро, не проверяя информацию, что может привести к раскрытию личных данных, установке вредоносного ПО или другим негативным последствиям. Пользователям важно развивать навыки распознавания таких методов и сохранять спокойствие при получении таких сообщений.

*11. Мобильные и социальные приложения:*

Некоторые приложения могут собирать и использовать личные данные без явного согласия пользователя, что может привести к манипуляции и нарушению конфиденциальности. Мобильные и социальные приложения: многие приложения собирают личные данные без явного согласия или ведома своих пользователей. Это может включать информацию о местоположении, контакты, всю историю использования и другие конфиденциальные данные. Злоумышленники могут использовать эти данные для целевых атак или манипуляций, а компании могут использовать их в рекламных целях или для продажи информации третьим лицам. Пользователи

должны внимательно прочитать условия использования, использовать настройки конфиденциальности и устанавливать только те приложения, которые им нужны, а также быть осторожными с разрешениями, которые запрашивают приложения.

Объект психологической манипуляции может привести к депрессии, самоубийству и трудностям в доверии к другим. Постоянные манипуляции и ложь создают эмоциональный стресс. Вследствие этого дети могут чувствовать себя растерянным и напряженным. Манипуляторы часто используют техники, которые заставляют их жертву чувствовать себя неполноценной. Это приводит к снижению самооценки и негативному влиянию на личность.

*Последствия негативного психоманипулятивного воздействия.*

- Психические расстройства: Увеличение случаев депрессии, тревожных расстройств и других психических заболеваний.
- Социальная изоляция: Постоянное воздействие киберугроз может привести к утрате доверия к окружающим и ухудшению социальных связей.
- Финансовые потери: Манипуляции могут привести к финансовым потерям, что также негативно сказывается на психическом состоянии.

В изучении моделей поведения в сфере кибербезопасности и их реализации сегодня по-прежнему доминируют технологические подходы. Эти методы зачастую направлены на разработку программного обеспечения, систем безопасности и других технических решений, направленных на предотвращение киберугроз. При этом психологические исследования в этой области остаются фрагментарными как по тематическому охвату, так и по конкретным результатам. Это создает существенные пробелы в понимании того, как поведение обучающихся в цифровой среде влияет на безопасность.

С ростом числа кибератак и утечек данных становится ясно, что чисто технологических решений недостаточно для полного обеспечения кибербезопасности. При постоянной или даже растущей актуальности этого вопроса на первый план выходит «психолого-педагогический фактор». Ошибки школьников - пользователей, неосведомленность о потенциальных угрозах и неосторожные действия в сети являются основными причинами многих инцидентов. Поэтому можно ожидать, что интерес к психологическим аспектам кибербезопасности в ближайшем будущем возрастет.

На смену заявлениям о недостаточной изученности этого вопроса приходит активное развитие психологических исследований, стремящихся к системному подходу. Сюда входит изучение факторов, способствующих формированию безопасного поведения пользователей, а также разработка программ и стратегий,

направленных на повышение осведомленности и ответственности в цифровом пространстве.

Портал психологических публикаций PsyJournals.ru предлагает актуальные материалы, которые помогут лучше разобраться в этих вопросах. Например, в статье «Психологические факторы кибербезопасности и доверия к фейковым новостям в интернет-коммуникации: обзор современных зарубежных исследований», опубликованной в журнале «Современная зарубежная психология», поднимаются важные аспекты взаимодействия пользователей с информацией в Интернете и их влияние на кибербезопасность. Такой подход помогает не только выявить основные психологические факторы, но и разработать рекомендации по повышению уровня кибербезопасности на индивидуальном и организационном уровнях.

Таким образом, интеграция психологических исследований в сферу кибербезопасности может привести к комплексному и эффективному решению проблемы с учетом как технологических, так и человеческих аспектов, что в свою очередь позволит создать безопасную цифровую среду для всех пользователей.

По этой причине и исходя из реальности ситуации вектор исследований, проводимых психологами, направлен на изучение вопросов психологической безопасности в профессиональной среде и педагогических коллективов, основного значения новых стратегий и методов киберпсихологии.

Важной научной задачей исследований в формате психологической науки является выявление ряда важных аспектов зарубежной научной мысли в плане понимания и обоснования роли психологической кибербезопасности в мобилизации психологических компонентов продуктивного ресурсного капитала в интересах эффективного решения стоящих перед школьным коллективом задач:

- во-первых, потенциала школьной команды в их высокоинтегрированной системе отношений, наличия;
- во-вторых, поиска новых резервов личностных качеств, соответствующих адекватному восприятию каждым членом коллектива своей миссии и проявления способности к практической реализации «командного духа» как главного условия сплоченности коллектива;
- в-третьих, роль школьного коллектива в обеспечении продуктивных условий процесса обучения.

Киберугрозы имеют многоуровневое влияние на психику человека. Понимание факторов негативного психоманипулятивного воздействия может помочь в разработке стратегий по защите от этих киберрисков и повышению осведомленности пользователей.

Киберриски в школьной среде могут оказывать значительное влияние на безопасность, конфиденциальность и психологическое

благополучие учащихся, преподавателей и административного персонала. Рассотрим основные киберриски в этой среде:

*Кибербуллинг:*

Описание: Учащиеся могут подвергаться агрессивному поведению со стороны сверстников через социальные сети, мессенджеры и другие онлайн-платформы.

Последствия: Это может привести к эмоциональному и психологическому стрессу, снижению успеваемости, и даже к более серьезным последствиям, таким как депрессия и суицидальные мысли.

*Фишинг и социальная инженерия:*

Описание: Ученики и сотрудники школы могут стать жертвами фишинговых атак, направленных на получение конфиденциальной информации, например, паролей и данных кредитных карт.

Последствия: В результате могут быть украдены личные данные, что приведет к финансовым потерям и нарушению приватности.

*Неавторизованный доступ к данным:*

Описание: Хакеры или даже учащиеся могут попытаться получить доступ к школьным информационным системам, чтобы изменить оценки, украсть личные данные или распространять вредоносное ПО.

Последствия: Это может повлиять на репутацию школы, нарушить образовательный процесс и поставить под угрозу конфиденциальность данных учащихся и сотрудников.

*Некачественное использование мобильных устройств:*

Описание: Учащиеся могут использовать мобильные устройства для доступа к несанкционированным или опасным веб-сайтам, скачивания вредоносных приложений или общения с незнакомцами.

Последствия: Это может привести к утечке личной информации, кибербуллингу или даже к вовлечению в опасные онлайн-группы.

*Вредоносное ПО и вирусы:*

Описание: Компьютеры и устройства, используемые в школьной сети, могут быть заражены вирусами и другими видами вредоносного ПО.

Последствия: Это может привести к утечке данных, сбоям в работе сети и оборудования, а также к необходимости восстанавливать системы, что потребует значительных ресурсов.

*Нарушение конфиденциальности данных:*

Описание: Учащиеся и сотрудники могут случайно или намеренно раскрыть конфиденциальные данные, такие как оценки, медицинские записи или личные данные.

Последствия: Это может привести к юридическим последствиям для школы, потере доверия со стороны родителей и учащихся, а также к возможным финансовым штрафам.

*Неэтичное использование социальных сетей:*

Описание: Учащиеся могут использовать социальные сети для распространения ложной информации, угроз, или для участия в опасных челленджах.

Последствия: Это может спровоцировать кризисы внутри школьного коллектива, ухудшение отношений между учащимися и негативное влияние на моральный климат в школе.

*Онлайн-груминг:*

Описание: Хищники могут использовать интернет и социальные сети для установления контакта с учащимися с целью их эксплуатации.

Последствия: Это представляет серьёзную угрозу для безопасности и благополучия учащихся, что требует немедленных мер реагирования со стороны школы и родителей.

Эти киберриски требуют внимательного подхода к вопросам кибербезопасности в школах, включая обучение учащихся и сотрудников основам цифровой грамотности и безопасности, внедрение защитных технологий и разработку политики использования интернет-ресурсов.

Для обнаружения киберрисков, как критически важного процесса для защиты цифровой инфраструктуры и данных в образовательных учреждениях, включая школы, существует несколько методов и подходов для выявления киберугроз и предотвращения киберинцидентов:

*1. Мониторинг сетевого трафика (Network Traffic Monitoring)*

Описание: Постоянный анализ входящего и исходящего сетевого трафика для выявления аномалий и подозрительных действий.

Примеры технологий: Системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), сетевые сенсоры.

Применение: В школах мониторинг сетевого трафика помогает обнаруживать подозрительную активность, такую как несанкционированный доступ или распространение вредоносного ПО.

*2. Анализ логов и событий (Log and Event Analysis)*

Описание: Сбор и анализ логов с различных систем и устройств (серверов, компьютеров, маршрутизаторов) для выявления аномалий и подозрительных действий.

Примеры технологий: SIEM (Security Information and Event Management) системы, централизованные системы сбора логов.

Применение: Анализ логов позволяет выявлять попытки несанкционированного доступа, сбои в системах безопасности и другие угрозы.

*3. Управление уязвимостями (Vulnerability Management)*

Описание: Регулярное сканирование сети на наличие уязвимостей в программном обеспечении, операционных системах и оборудовании.

Примеры технологий: Сканеры уязвимостей (например, Nessus, OpenVAS), тестирование на проникновение (penetration testing).

Применение: Управление уязвимостями помогает своевременно выявлять и устранять слабые места в системе, предотвращая возможные атаки.

*4. Анализ поведения пользователей и сущностей (UEBA – User and Entity Behavior Analytics)*

Описание: Использование машинного обучения и поведенческого анализа для выявления аномалий в поведении пользователей и устройств.

Примеры технологий: Системы UEBA, интегрированные с SIEM.

Применение: В школах это может использоваться для обнаружения подозрительных действий учащихся или сотрудников, например, необычно большой объем скачанных данных или попытки доступа к конфиденциальной информации.

*5. Песочницы и изоляционные среды (Sandboxing)*

Описание: Изоляция подозрительных файлов и программ в виртуальной среде для анализа их поведения.

Примеры технологий: Песочницы для анализа вредоносного ПО (например, Cuckoo Sandbox).

Применение: Песочницы позволяют безопасно анализировать подозрительные файлы или вложения, что помогает предотвратить распространение вирусов и другого вредоносного ПО.

*6. Обнаружение аномалий с помощью ИИ и машинного обучения*

Описание: Использование искусственного интеллекта для анализа большого объема данных и выявления аномальных паттернов, которые могут свидетельствовать о киберугрозах.

Примеры технологий: ИИ-инструменты, встроенные в SIEM системы, автономные решения для обнаружения аномалий.

Применение: В образовательных учреждениях ИИ может помочь автоматизировать процесс обнаружения угроз и снизить вероятность пропуска важных инцидентов.

*7. Проверка целостности файлов и систем (File Integrity Monitoring)*

Описание: Мониторинг изменений в ключевых файлах и конфигурациях системы для обнаружения несанкционированных изменений.

Примеры технологий: Tripwire, OSSEC.

Применение: Эта технология помогает обнаруживать попытки взлома или несанкционированного доступа к критически важным системам школы.

*8. Тестирование на проникновение (Penetration Testing)*

Описание: Имитация кибератак для проверки защищенности систем и выявления потенциальных уязвимостей.

Примеры технологий: Ручное тестирование, автоматизированные инструменты (например, Metasploit).

Применение: Регулярное проведение тестов помогает обнаруживать слабые места в безопасности и улучшать защиту до того, как их смогут использовать злоумышленники.

*9. Кибербразведка (Cyber Threat Intelligence)*

Описание: Сбор и анализ информации о текущих и потенциальных киберугрозах из различных источников, включая форумы, темные веб-ресурсы и специализированные базы данных.

Примеры технологий: Платформы кибербразведки, такие как Recorded Future, Mandiant.

Применение: Школы могут использовать информацию о новых угрозах и уязвимостях для своевременного обновления своих систем безопасности.

*10. Фишинг-тесты и обучение персонала*

Описание: Проведение учебных фишинговых атак и обучение сотрудников и учащихся основам кибербезопасности.

Примеры технологий: Платформы для обучения кибербезопасности, такие как KnowBe4.

Применение: Помогает повысить осведомленность и готовность персонала и учащихся к возможным кибератакам.

Эти методы позволяют школам и другим образовательным учреждениям своевременно обнаруживать и реагировать на киберугрозы, минимизируя потенциальные риски и защищая свои данные и системы.

Рекомендации:

- Образование и повышение осведомленности о киберугрозах.
- Разработка программ психологической поддержки для жертв кибербуллинга и манипуляций.
- Создание безопасной онлайн-среды путем регулирования контента и защиты личных данных.

Факторы негативного психоманипулятивного воздействия киберугроз представляют собой сложное и многослойное явление, оказывающее прямое влияние на психическое, социальное и эмоциональное благополучие школьников. Рассмотренные примеры — от дезинформации и социальной инженерии до кибербуллинга, токсичной среды в социальных сетях и эмоционального давления — демонстрируют, что подростки особенно уязвимы из-за недостаточного опыта, доверчивости и ограниченных навыков критической оценки информации. Наличие таких угроз приводит к росту тревожности, снижению самооценки, формированию зависимостей и риску социальных и учебных дезадаптаций.

В то же время анализ факторов указывает на необходимость системного подхода, объединяющего технологические, психологические и педагогические меры. Техническая защита сама по себе не способна предотвратить манипулятивные практики — требуется формирование у школьников цифровой грамотности, устойчивости к психологическим воздействиям и навыков ответственного поведения в сети. Комплексная профилактика, включающая образовательные программы, психологическую поддержку и развитие критического мышления, становится ключевым условием создания безопасной образовательной среды, способной минимизировать негативное влияние киберугроз и обеспечить гармоничное развитие личности в цифровом обществе.

## 1.4 Диагностический инструментарий для измерения цифровой грамотности, степени тревожности и напряженности субъектов школьной образовательной среды

Несмотря на то, что современные школьники часто именуются «цифровыми аборигенами» или представителями «сетевого поколения» – ведь они фактически выросли в цифровой среде – даже им необходимо знакомство с новыми возможностями и угрозами онлайн-пространства. Им требуются специальные компетенции, чтобы эффективно удовлетворять информационные запросы и ориентироваться в правилах поведения в цифровой среде.

На сегодняшний день цифровая грамотность признана одной из ключевых навыков XXI века, актуальных практически для любой профессии. Ее востребованность сравнивается с традиционными навыками чтения и письма: как отметил директор Mozilla Foundation, “понимание того, как работают цифровые технологии, равноценно чтению, письму и математике” [64].

Обзор широкого спектра научных публикаций, посвященных глобализации образовательных процессов, внедрению ИКТ и цифровой трансформации отечественного образования, показывает, что термин “digital literacy” активно используется как в отечественной, так и в зарубежной педагогике.

С начала XXI века ведущие зарубежные исследователи – такие как П. Гилстер, Г. Дженкинс, М. Варшавер, Т. Матучняк, А. Мартин, Е. Харгитай и др. – сформулировали концепцию цифровой грамотности как интеграции когнитивных, социальных и технических умений для полноценного функционирования в информационной среде.

Со временем цифровая грамотность стала трактоваться как более сложное и многоаспектное понятие, включающее в себя:

- владение техническими средствами (компьютерами, программами);

– умение искать, анализировать и критически осмысливать информацию;

– компетентное использование социальных медиа;

– работа в сети с пониманием сетевой безопасности и норм сетевого этикета.

Современные подходы дополнительно подчеркивают важность экопсихологического аспекта: здорового отношения к цифровым технологиям, включая цифровую гигиену и ответственность.

Цифровая грамотность зависит от формирования трех ключевых типов навыков:

1. работы с устройствами доступа к интернету (компьютеры, смартфоны и т.п.);
2. взаимодействия с программным обеспечением для работы с контентом;
3. универсальных навыков создания и организации цифровой (онлайн-/офлайн-) среды;
4. сохранение экопсихологических ресурсов и развитие креативного мышления.

Особое внимание заслуживает определение Д. Белшоу в его работе «Основные элементы цифровой грамотности», в котором он выделяет восемь ключевых компонентов успешного цифрового взаимодействия [65].

– Культурный компонент – способность понимать контекст различных цифровых сред (ценности, символы, сетевой этикет), а также различать личное и профессиональное в цифровом пространстве.

– Когнитивный компонент – знание основ компьютерной грамотности, меню, тегов, хэштегов, что упрощает навигацию и использование интерфейсов.

– Конструктивный компонент – умение создавать новый контент, включая преобразование или ремикс существующих материалов с уважением к авторским правам.

– Коммуникативный компонент – знание особенностей цифрового общения, концепций идентичности, доверия и влияния в информационном обмене.

– Уверенное использование (Confident) – ощущение себя частью онлайнового сообщества и готовность использовать цифровые возможности для обучения и творчества.

– Креативность – способность использовать цифровые инструменты для создания нового знания или продуктов.

– Критический компонент – умение оценивать цифровой контент, инструменты и источники с точки зрения надежности и ценности.

– Гражданский компонент – способность использовать цифровые средства для самоорганизации, защиты цифровых прав и участия в онлайн-гражданской активности [65].

Как подчеркивают зарубежные ученые, важно помогать учащимся становиться более осторожными и осознанными пользователями интернет-информации, обучая их критически относиться к контенту и быть грамотными в обращении с личными данными [66].

Определения цифровой грамотности звучит так: «это знания, установки и умения правильно использовать цифровые инструменты для идентификации, доступа, управления, анализа и синтеза цифровых ресурсов, создания новых знаний, медиа-сообщений и общения в конкретных жизненных ситуациях, с целью конструктивного социального взаимодействия и рефлексии» [67].

В отечественной литературе в последние годы цифровая грамотность активно обсуждается и критикуется многими исследователями.

Анализ существующих исследований в области цифровой грамотности позволил сделать вывод, что при большой распространенности трактовка понятия «цифровая грамотность» достаточно неоднозначна. Различные источники определяют цифровую грамотность как способность, набор знаний, умений, навыков и т.п.

Термин «digital literacy» был впервые введен П. Гилстером в одноименной монографии [69], где автор определил его как «способность понимать и использовать информацию в самых разных форматах, получаемую с помощью компьютеров и сети Интернет». Таким образом, изначально акцент делался на умении находить, интерпретировать и критически оценивать цифровой контент.

Позднее концепция цифровой грамотности была развита в трудах Е. Харгитай [70], которая подчеркнула различия в уровне владения цифровыми инструментами среди разных социальных групп, выделив социальное измерение цифрового неравенства. В свою очередь, Д. Белшоу [65] предложил рассматривать цифровую грамотность через восемь ключевых элементов: культурный, когнитивный, конструктивный, коммуникативный, конфидентный, креативный, критический и гражданский. Этот подход позволил расширить категорию до комплексной компетенции, охватывающей личностные, когнитивные и социокультурные аспекты.

*2. Структура и ключевые компоненты цифровой грамотности*

В современном дискурсе цифровая грамотность трактуется как совокупность навыков и умений, включающая три основных уровня:

1. Технический уровень – базовые умения работы с цифровыми устройствами, программами, сетевыми ресурсами.

2. Информационный уровень – способность к поиску, анализу, критической оценке и использованию информации.

3. Социально-коммуникативный уровень – умение взаимодействовать в цифровой среде, соблюдать нормы этики и безопасности, осознавать последствия цифровых действий.

Таким образом, цифровая грамотность выступает как многоуровневая компетенция, включающая в себя как инструментальные, так и метапознавательные характеристики.

Несмотря на близость, перечисленные термины отражают разные аспекты владения технологиями. Компьютерная грамотность (computer literacy) в традиционном понимании ограничивается умением управлять файлами, работать с офисными приложениями, знать основы информатики. Информационная грамотность (information literacy) связана с умением искать и критически оценивать информацию. ИКТ-компетентность трактуется как способность использовать информационно-коммуникационные технологии в образовательной и профессиональной деятельности.

Как подчеркивает Н.Д. Берман в статье «К вопросу о цифровой грамотности» [71], цифровая грамотность (digital fluency) отличается большей комплексностью: она включает «набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий, интернет-ресурсов и собственных человеческих ресурсов».

В условиях цифровизации образования цифровая грамотность становится необходимым условием успешной профессиональной и личностной самореализации. Она обеспечивает способность обучающихся к критическому восприятию информации, формирует навыки ответственного поведения в сети, способствует развитию креативности и медиакомпетентности.

В казахстанской образовательной политике развитие цифровой грамотности рассматривается как стратегическая задача. В частности, в рамках государственной программы «Цифровой Казахстан» акцент делается на формирование у школьников и студентов цифровых компетенций, необходимых для интеграции в глобальное информационное пространство [72].

По мнению С.В. Гайсиной [73] «отличием цифровой грамотности от ИКТ-компетентности является кибербезопасность и безопасность в сети Интернет, как умение оценить достоверность информации, как умение сохранить свои личные и персональные данные, умение защитить себя. Об этом мы говорили и раньше, но в условиях цифровизации образования эта компетентность становится более значимой, чем ранее, составляющей цифровой грамотности и цифровой компетентности».

Феномен цифровой грамотности изучается - это основа безопасности в информационном обществе. Формированию цифровой

грамотности должно уделяться особое внимание наравне с не только читательской, математической и естественнонаучной грамотностью, но и безопасно себя сохранят во всех сферах жизнедеятельности» и от социопсихологические угрозы (социальные, этические, психологические аспекты работы в цифровой среде)»

С распространением интернета в научно-педагогическом дискурсе стали активно использоваться термины «интернет-культура» и «интернет-грамотность», обозначающие формы поведения и навыков, специфичные для сетевой среды. В дальнейшем эти понятия развились в более широкое представление, представленное термином «электронная культура» (*e-culture* или «цифровая культура»), отражающий комплекс цифровых коммуникаций, технологий, сетевых практик и ценностей, присущих информационному обществу [74].

Развитие этих понятий послужило основаниям для закрепления идеи о цифровой грамотности как ключевой компетенции современного общества. В этой связи особо примечательны исследования А. В. Шарикова, который в своих работах предлагает концептуальное различение подходов к цифровой грамотности, организуя их вокруг двух осей оппозиций. В одной из своих статей он выделяет четыре фундаментальных компонента, отражающих различие между технологическими и социогуманитарными аспектами, а также между возможностями и угрозами цифровой среды: технико-прагматические возможности, содержательно-коммуникативные возможности, технико-технологические угрозы и социопсихологические угрозы [75].

В данной модели:

- Содержательно-коммуникативные подходы акцентируют внимание на создании и восприятии медиатекстов, умении взаимодействовать в цифровых сообществах и понимать смысл содержания.
- Технико-технологические подходы сосредоточены на технических навыках использования браузеров, облачных технологий, инструментов хранения и передачи данных.
- Социогуманитарный аспект связан с вопросами цифровой безопасности, этического поведения и социально-психологических рисков работы в сети.

Таким образом, цифровая грамотность в понимании Шарикова – это многосоставной феномен, охватывающий и техническую обусловленность, и коммуникативную значимость, а также должно учитывать потенциальные угрозы цифровой среды и социально-психологические последствия ее использования.

Рассматриваются такие компоненты цифровой компетентности как знания, умения, мотивация и ответственность в разных сферах деятельности в интернете (работа с контентом, коммуникация,

техносфера, потребление); показывается необходимость учета как отношения школьников к интернету, так и особенностей его деятельности».

Нам представляется более правильным и точным относительно школьников говорить, прежде всего, о цифровой грамотности, на основе которой будет формироваться цифровая компетентность обучающегося.

Таким образом, исследователи рассматривают цифровую грамотность как феномен в пределах культурологии, социологии, психологии процессов информатизации в образовании.

При разработке проекта в сфере образования необходимо:

1) внедрить на уровнях основного общего и среднего общего образования новые методы обучения и воспитания, образовательные технологии, обеспечивающие освоение обучающимися базовых навыков и умений и повышающие их мотивацию к обучению;

2) создать современную и безопасную цифровую образовательную среду, обеспечивающую высокое качество и доступность образования всех видов и уровней в формате единого федерального образовательного пространства.

Критерии оценивания описывают системные наборы важных качеств, заключающихся в продуктах обучения. Термин «критерии оценивания» используется только учителями в профессиональной среде, в отчетах, методических работах, статьях и т.д.

Для учащихся формулируются критерии успеха – доступно, кратко, используя глаголы, обычно 1 лица единственного числа (таблица 1.4.1).

Таблица 1.4.1 – Система критериев успеха

| Критерии успеха (для учащихся) | Критерии оценивания (для учителей) |
|---|---|
| 1. Знаю название и автора стихотворения. | 1. Знает название и автора стихотворения. |
| 2. Воспроизвожу весь текст. | 2. Воспроизводит весь текст. |
| 3. Четко и правильно произношу слова. | 3. Четко и правильно произносит слова |

Таким образом, школьнику обеспечиваются условия для выстраивания достиженческого поведения в комфортном для него ритме и в индивидуальном контексте формирования личности.

Для детей с особыми образовательными потребностями используется та же критериальная система оценивания, но на основе индивидуального учебного плана.

И далее определены дескрипторы базовых понятий кибербезопасности в свете современного состояния проблемы и

системообразующих признаков безопасной образовательной среды, включающие дескрипторы по направлениям «угрозы и риски», «уязвимости», «обнаружение инцидентов», «защита», «политика безопасности», «киберэтика».

Анализ уязвимостей: концептуальное содержание и практическое значение в информационной безопасности

Анализ уязвимостей – это методологически выстроенный процесс, направленный на выявление потенциальных угроз, слабых звеньев и рисков несанкционированного вторжения злоумышленников в информационную систему (ИС). Под уязвимостью понимают компонент, обладающий недостаточной защищенностью, будь то программное обеспечение, аппаратная платформа или человеческий фактор, которые могут быть использованы злоумышленниками [76].

Угроза, в свою очередь, – это потенциальное событие или действие, способное использовать уязвимость и нанести вред целостности, конфиденциальности или доступности информации.

В этой модели злоумышленник играет роль агента угрозы, намеренно или случайно реализующего негативное воздействие.

Наличие уязвимостей снижает устойчивость организации: она становится уязвимой перед конкурентами, злоумышленники получают упрощенный доступ к критически важной информации. При этом источники угроз могут быть различными – преднамеренными, непреднамеренными, а также техногенными или природными.

Современный подход к анализу уязвимостей включает детальное выявление конкретной уязвимости для каждой угрозы, что позволяет выявлять пути ее реализации.

*Аудит ИБ и охват ключевых рисков*

В рамках аудита информационной безопасности проводится анализ уязвимостей, который обеспечивает не только защиту от утечек данных, но и финансовую стабильность организации. В современном бизнес-контексте предприятия стремятся к предотвращению:

- утечек корпоративной информации;
- несанкционированного редактирования;
- снижения доверия со стороны партнеров и инвесторов.

Ключевыми являются четыре базовых принципа ИБ: конфиденциальность, целостность и доступность – традиционно называемые триадой "CIA", а также достоверность, обозначаемая в ряде источников как еще один критически важный компонент (иногда расширяемый до пятого принципа аутентичности) [77].

*Классификация угроз*

Качественный анализ уязвимостей требует системного подхода к классификации угроз:

1. Класс 1 (источник угрозы):

– внутри ИС;
– в пределах видимости (например, устройства для записи);
– вне зоны видимости (например, возможность перехвата данных в сети).

2. Класс 2 (характер воздействия):
– активные атаки (вредоносное ПО);
– пассивный доступ к информации (скопировать данные без вмешательства).

3. Класс 3 (способ реализации):
– прямые методы (кража паролей);
– косвенные (уязвимости ОС, нестандартные каналы).

Главные цели атак – контроль над ресурсами, несанкционированный доступ к корпоративной сети, подрыв функционирования компании.

*Оценка вероятности угроз*

Вероятность реализации угрозы классифицируется по качественной шкале:

1. Низкая (Н) – крайне редкие события, например, раз в 5–10 лет;
2. Средняя (С) – угрозы с известными предпосылками, реализация примерно раз в год;
3. Высокая (В) – частые атаки, подтвержденные инцидентами, статистикой.

*Методики анализа и превентивные меры*

Основные методы анализа уязвимостей основаны на вероятностной оценке и учитывают следующие аспекты: потенциал злоумышленника, источник угрозы, метод воздействия и объект атаки.

Ключевой компонент защиты – оперативное обнаружение и устранение уязвимостей в ОС и ПО, установка патчей и конфигураций безопасности (vulnerability management) [78].

Регулярный анализ настроек защитных средств, настройка непрерывного мониторинга и управление доступом существенно повышают устойчивость информационной системы. ИБ также предусматривает ограничение прав доступа, контроль установки ПО и использование внешних носителей.

*«Обнаружение инцидентов».*

Политика реагирования на инциденты ИБ разрабатывается с учетом специфики организации, профиля ее деятельности. В большинстве организаций процесс управления инцидентами ИБ построен следующим образом:

– получение информации об инциденте;
– получение дополнительной информации, связанной с выявленным инцидентом;

– анализ ситуации, локализация инцидента и оперативное применение контрмер;

– установление причин, по которым стал возможен инцидент, и определение ответственных лиц (расследование);

– проведение корректирующих и профилактических мероприятий.

Основными задачами, решаемыми с помощью технических средств и систем выявления инцидентов ИБ, являются:

– осуществление централизованного сбора, обработки и анализа событий из множества распределенных гетерогенных источников событий;

– обнаружение в режиме реального времени атак, вторжений, нарушений политик безопасности;

– контроль за портами и устройствами ввода/вывода информации;

– мониторинг действий пользователей;

– предоставление инструментария для проведения расследований инцидентов ИБ, формирования доказательной базы по инциденту ИБ.

Кибернетическую безопасность также следует рассматривать как часть духовной, а именно информационно-психологической безопасности и, придавая ей значение как одной из важнейших в современных условиях, характеризующихся собой состояние защищенности от внутренних и внешних угроз кибернетического пространства социума, средств массовой коммуникации военного, общегосударственного и гражданского назначения, а также общественного сознания как одного из основных национальных информационных ресурсов.

Таким образом, политика кибербезопасность, как и регулируемая ею сфера отношений -киберпространство, также имеет две содержательных составляющих - информационную сторону и техническую, что кардинально, существенно расширяет область ее действия и выводит за рамки безопасности собственно информационной.

Система критериев и дескрипторов уровней цифровой грамотности, включающая пять ключевых компонентов (информационная грамотность, компьютерная грамотность, медиаграмотность, коммуникативная грамотность и технологические инновации), позволит оценивать уровень владения этими навыками у различных групп пользователей, таких как учащиеся, учителя и родители. Рассмотрим систему по каждому из компонентов [79, 80].

Эта система критериев и дескрипторов уровней цифровой грамотности позволяет более детально оценить и развивать ключевые компетенции в цифровом мире. Использование этой структуры

поможет эффективно обучать и повышать уровень цифровой грамотности среди различных групп участников образовательного процесса, а также даст четкие ориентиры для планирования образовательных программ и тренингов.

С учетом всего сказанного были составлены 2 анкеты для учителей средних общеобразовательных школ, одну из которых мы приводим здесь (таблица 1.4.2), вторая анкета, а также анкета для родителей и учащихся школ отражена на сайте проекта https://cyberacademy.ppu.edu.kz/.

Таблица 1.4.2 – Индекс цифровой грамотности

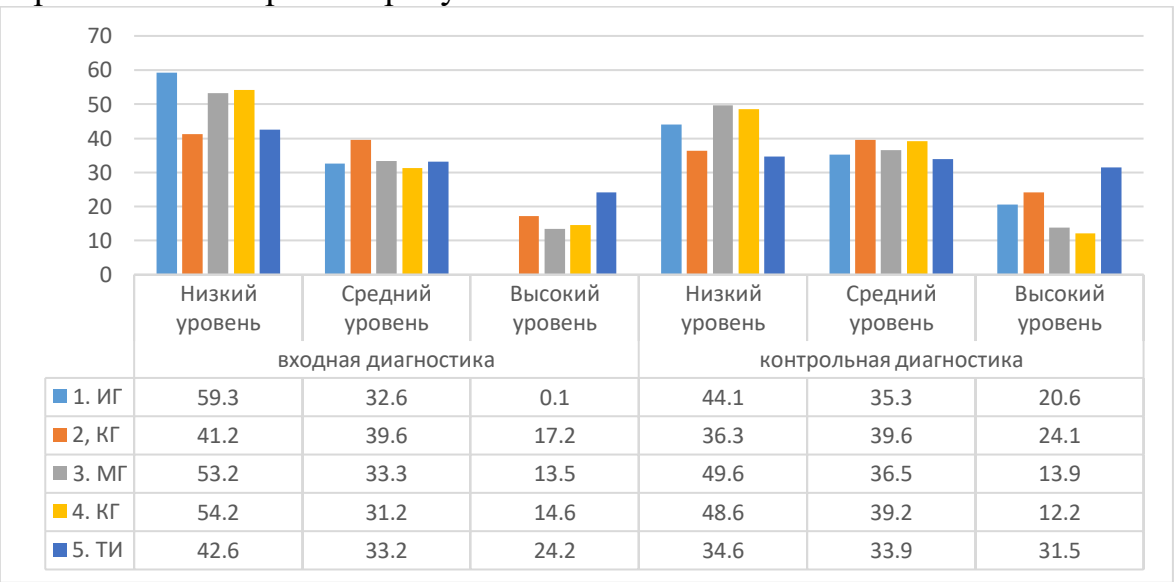
| Компоненты ЦГ | Критерии ЦГ | Уровни и индикаторы | |
|---|---|---|---|
| | | Оптимальный уровень | Критический уровень |
| Информационная грамотность | Знания о специфике информации и различных ее источниках | Делаю выводы на основе информации из разных источников | Доверяю одному источнику информации |
| | Навыки поиска релевантной информации и ее сравнения | С легкостью могу найти информацию в интернете | Мне сложно найти нужную информацию в интернете |
| | Установки в отношении пользы и вреда информации | Регулярно задумываюсь над тем, насколько полезна или вредна информация, которую я получаю в интернете | Не задумываюсь о полезности или вреде информации, которую я получаю в интернете |
| Компьютерная грамотность | Знание устройства компьютера и его функций | Могу оценить, насколько современные компьютер и программное обеспечение я использую | Мне сложно оценить, насколько компьютер и ПО современны |
| | Навыки использования компьютера и аналогичных устройств | Для меня работа на компьютере – это естественный процесс, не вызывающий затруднений | Мне сложно и непривычно работать на компьютере |
| | Установки в отношении роли компьютера в ежедневной | Компьютер помогает мне в решении повседневных | Компьютер нужен мне скорее для развлечений и досуга |

| | | | |
|---|---|---|---|
| | практике | задач для работы, учебы и т.д. | |
| Медиаграмотность | Знание о медиа-контенте и его источниках | Я сравниваю разные источники новостей, чтобы удостовериться в правдивости освещения СМИ разных событий | Я не подвергаю сомнению новости из СМИ, которым я доверяю |
| | Навыки поиска новостей и фактчекинга | Я знаю, как всегда быть в курсе последних событий и новостей | Мне сложно ориентироваться в потоке новостей и событий |
| | Установки в отношении достоверности информации, сообщаемой через СМИ | Я считаю, что СМИ, которые я предпочитаю, могут сообщать неполную информацию либо преподносить ее в выгодном кому-то свете | Я считаю, что СМИ, которым я доверяю, полно, непредвзято и правдиво освещают происходящие события |
| Коммуникативная грамотность | Знания о специфики диалога в цифровой коммуникации | Обычно я анализирую позицию своего собеседника (-ов) в интернете | Я редко анализирую позицию своего собеседника (собеседников) в интернете |
| | Навыки использования современных средств коммуникации | Я свободно могу использовать современные средства коммуникации (мессенджеры, социальные сети) | Для меня непривычно и неестественно использовать современные средства коммуникации (мессенджеры, социальные сети) для общения |
| | Установки в отношении этики и норм общения в цифровой среде | Я считаю, что в интернете должны соблюдаться такие же нормы общения, как в реальной жизни | Я считаю, что обычные нормы общения не подходят для интернета – здесь можно общаться свободно |
| Технологические инновации | Знания современных технологических тенденций | Я стараюсь быть в курсе технологических новинок, слежу за трендами | Я не отслеживаю новинки и тренды в сфере технологий |

| | | | |
|---|---|---|---|
| | Навыки работы с гаджетами и приложениями | Использование современных технологий не вызывает у меня затруднений | Мне сложно осваивать современные технологии |
| | Установки в отношении пользы технологических инноваций | Современные гаджеты и приложения помогают в повседневной жизни | Гаджеты и приложения мешают, отвлекают меня от важных дел |

В данной части нашей монографии мы приводим результаты применения всего диагностического инструментария, который был использован дважды: до опытно-педагогической работы и после. Детально не останавливаясь на всех диагностических процедурах и данных, мы посчитали уместным изложить отдельные фрагменты, которые отражают ключевые тенденции.

Полученные результаты по итогам входной и контрольной диагностик представлены по следующим группам: 5-7 классы (159 человек), 8-9 классы (162 человека), 10-11 классы (101 человек) отражены в материалах рисунков 1.4.1-1.4.4.




| | входная диагностика | | | контрольная диагностика | | |
|---|---|---|---|---|---|---|
| | Низкий уровень | Средний уровень | Высокий уровень | Низкий уровень | Средний уровень | Высокий уровень |
| 1. ИГ | 59.3 | 32.6 | 0.1 | 44.1 | 35.3 | 20.6 |
| 2, КГ | 41.2 | 39.6 | 17.2 | 36.3 | 39.6 | 24.1 |
| 3. МГ | 53.2 | 33.3 | 13.5 | 49.6 | 36.5 | 13.9 |
| 4. КГ | 54.2 | 31.2 | 14.6 | 48.6 | 39.2 | 12.2 |
| 5. ТИ | 42.6 | 33.2 | 24.2 | 34.6 | 33.9 | 31.5 |

Рисунок 1.4.1 – Показатели динамики сформированности цифровой грамотности, степени тревожности и напряженности субъектов школьной образовательной среды, вызванных киберопасностью: 5-7 классы (в%)

Диаграмма (рисунок 1.4.1) демонстрирует динамику уровня цифровой грамотности учащихся 5–7 классов в сопоставлении с показателями тревожности и напряженности, вызванными киберугрозами. Наиболее отчетливо прослеживается зависимость: чем выше степень сформированности цифровых компетенций, тем ниже

выражены эмоциональные состояния дезадаптивного характера. Это закономерно, поскольку овладение инструментами безопасного поведения в сети снижает неопределенность и способствует повышению уверенности подростков в собственных действиях.

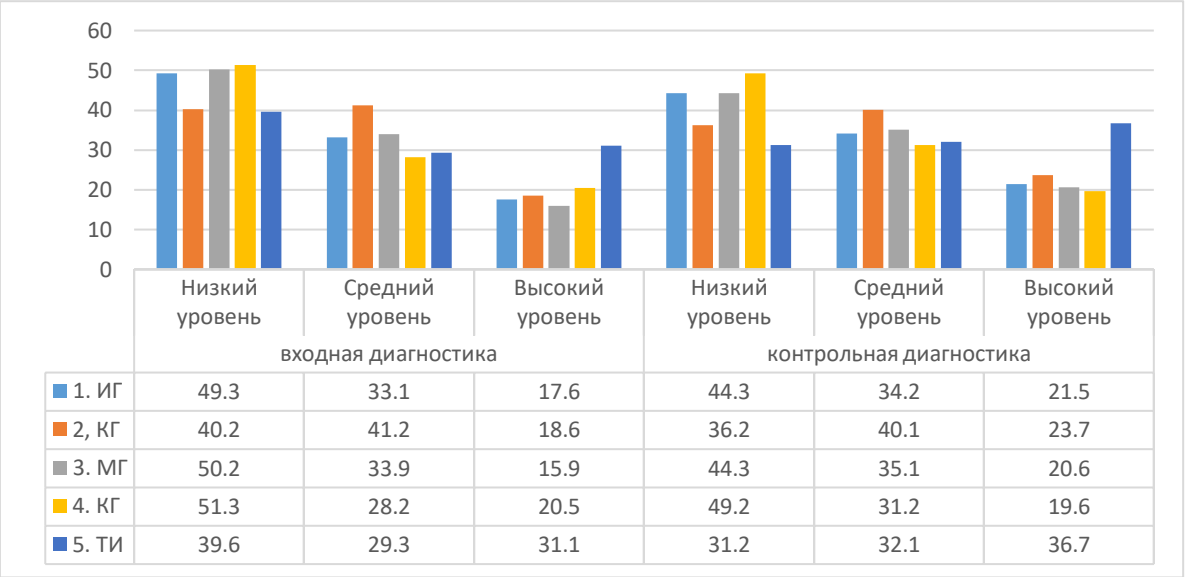
Анализ данных показывает, что в 5-х классах отмечается наиболее низкий уровень цифровой грамотности при высокой степени тревожности и напряженности. Данный факт свидетельствует о недостаточной подготовленности младших подростков к самостоятельному взаимодействию с цифровой средой, что влечет за собой повышенную восприимчивость к киберугрозам. В 6-х классах показатели постепенно выравниваются: уровень цифровых компетенций возрастает, а эмоциональное напряжение снижается. В 7-х классах формируется относительное равновесие – рост цифровой грамотности сопровождается заметным снижением тревожности, что подтверждает эффективность естественного накопления опыта и, вероятно, педагогических мероприятий по формированию ИКТ-компетентности.

Таким образом, полученные результаты подтверждают наличие обратной корреляции между уровнем цифровой грамотности и степенью эмоциональной уязвимости учащихся. Сформированность цифровых компетенций выступает не только образовательным, но и психопрофилактическим фактором, снижая риски деструктивного влияния киберопасностей на

С методологической точки зрения представленная динамика подчеркивает необходимость целенаправленного формирования цифровой грамотности уже на этапе среднего звена школы. Педагогическая практика должна не ограничиваться передачей технических знаний, но включать элементы психологической подготовки, формирование навыков критического мышления и саморегуляции в условиях киберрисков.

Для 5-х классов приоритетным направлением становится базовое обучение безопасному использованию цифровых ресурсов, а также работа с эмоциональной сферой через игровые формы, тренинги и профилактические беседы. В 6-х классах акцент можно смещать в сторону проектной деятельности и самостоятельного поиска информации, что укрепляет уверенность учащихся в цифровой среде. В 7-х классах уже возможна интеграция междисциплинарных модулей (например, информатика + обществознание + психология), где цифровая грамотность рассматривается как часть общей культуры личности.

Таким образом, выявленные закономерности позволяют разрабатывать адаптированные образовательные программы, направленные на снижение тревожности школьников и укрепление их психологической устойчивости за счет последовательного и поэтапного развития цифровых компетенций.




| | входная диагностика | | | контрольная диагностика | | |
|---|---|---|---|---|---|---|
| | Низкий уровень | Средний уровень | Высокий уровень | Низкий уровень | Средний уровень | Высокий уровень |
| 1. ИГ | 49.3 | 33.1 | 17.6 | 44.3 | 34.2 | 21.5 |
| 2, КГ | 40.2 | 41.2 | 18.6 | 36.2 | 40.1 | 23.7 |
| 3. МГ | 50.2 | 33.9 | 15.9 | 44.3 | 35.1 | 20.6 |
| 4. КГ | 51.3 | 28.2 | 20.5 | 49.2 | 31.2 | 19.6 |
| 5. ТИ | 39.6 | 29.3 | 31.1 | 31.2 | 32.1 | 36.7 |

Рисунок 1.4.2 – Показатели динамики сформированности цифровой грамотности, степени тревожности и напряженности субъектов школьной образовательной среды, вызванных киберопасностью: 8-9 классы (в%)

Анализ представленных данных показывает, что у учащихся 8–9 классов уровень цифровой грамотности в целом выше, чем у младших подростков (5–7 классы). Это закономерно, так как к данному возрасту школьники приобретают больше опыта самостоятельного использования информационных технологий и обладают более развитыми когнитивными навыками. Однако одновременно наблюдается усиление тревожности и напряженности, связанной с киберугрозами.

Такой парадокс объясняется расширением цифровой активности подростков: они чаще взаимодействуют в социальных сетях, используют онлайн-сервисы для учебы и общения, сталкиваются с проблемами кибербуллинга, фишинга, нежелательного контента и другими проявлениями цифровых рисков. Чем выше интенсивность погружения в интернет-пространство, тем больше осознание уязвимости и возможных угроз.

Методологически это подтверждает, что цифровая грамотность в подростковом возрасте не всегда выступает защитным фактором. Если у учащегося отсутствует психологическая устойчивость и навыки ответственного поведения в сети, знание технологий само по себе может лишь усиливать тревожность (эффект «осведомленности об опасности»).

*Методологические выводы*

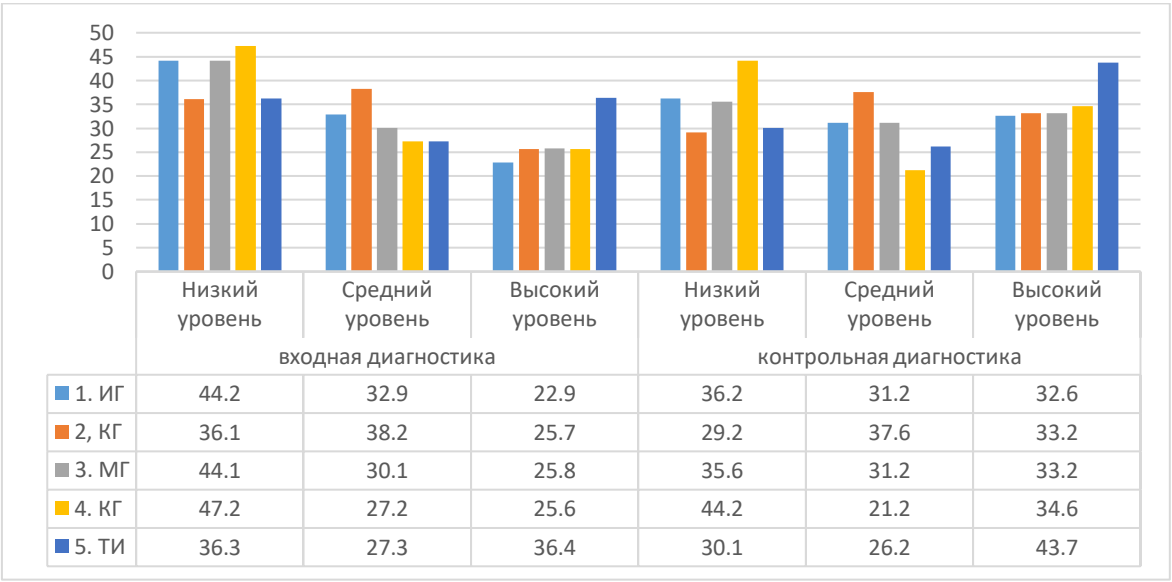
– Для 8 классов ключевым направлением работы становится развитие критического мышления: умение оценивать достоверность

информации, различать безопасный и небезопасный цифровой контент.

– Для 9 классов важно формировать ответственное цифровое поведение и устойчивость к психологическому давлению в сети (например, противостояние кибербуллингу, защита персональных данных, цифровая гигиена).

– В сравнении с 5–7 классами акцент смещается с «обучения базовым техническим навыкам» на углубленное освоение этических, правовых и психологических аспектов цифровой грамотности.

Таким образом, данные диаграммы подчеркивают, что в старшем подростковом возрасте требуется комплексный подход: наряду с технической подготовкой необходимо систематически включать в образовательные программы психолого-педагогические практики, ориентированные на снижение тревожности и формирование позитивной цифровой идентичности.




| | Низкий уровень | Средний уровень | Высокий уровень | Низкий уровень | Средний уровень | Высокий уровень |
|---|---|---|---|---|---|---|
| | входная диагностика | | | контрольная диагностика | | |
| 1. ИГ | 44.2 | 32.9 | 22.9 | 36.2 | 31.2 | 32.6 |
| 2, КГ | 36.1 | 38.2 | 25.7 | 29.2 | 37.6 | 33.2 |
| 3. МГ | 44.1 | 30.1 | 25.8 | 35.6 | 31.2 | 33.2 |
| 4. КГ | 47.2 | 27.2 | 25.6 | 44.2 | 21.2 | 34.6 |
| 5. ТИ | 36.3 | 27.3 | 36.4 | 30.1 | 26.2 | 43.7 |

Рисунок 1.4.3 – Показатели динамики сформированности цифровой грамотности, степени тревожности и напряженности субъектов школьной образовательной среды, вызванных киберопасностью: 10-11 классы (в%)

Анализ показателей (рисунок 1.4.3) демонстрирует, что в старшей школе (10–11 классы) цифровая грамотность достигает наиболее высокого уровня по сравнению с младшими возрастными группами. Старшеклассники уверенно владеют устройствами, программным обеспечением, навыками поиска и критической обработки информации, активно используют сетевые платформы для учебы, самореализации и коммуникации. Важной особенностью данного периода является осознание учащимися правовых и этических аспектов цифрового взаимодействия: они лучше понимают

ценность персональных данных, начинают проявлять избирательность к источникам информации, а также формируют более устойчивую цифровую идентичность.

*Тревожность.* Несмотря на высокий уровень цифровой грамотности, степень тревожности остается достаточно значимой. Однако природа этой тревожности меняется: она связана не столько с техническими ошибками или незнанием правил, сколько с социально-психологическими рисками. Подростки старшего школьного возраста сталкиваются с проблемами, связанными с публичностью в сети, угрозой репутационных потерь, воздействием кибербуллинга, интернет-зависимости или манипулятивных практик в цифровой среде. Таким образом, тревожность приобретает более сложный, экзистенциальный характер, связанный с личной и социальной идентичностью учащихся.

*Напряженность.* Показатели напряженности в 10–11 классах также остаются заметными, хотя носят иной характер по сравнению с младшими школьниками. Если у подростков 5–7 и 8–9 классов напряженность во многом была связана с техническими трудностями и первоначальной адаптацией к рискам, то у старшеклассников она определяется сочетанием учебных, социальных и психологических факторов. На первый план выходит необходимость балансировать между интенсивным использованием цифровых ресурсов для учебы (подготовка к экзаменам, участие в олимпиадах, онлайн-курсы) и поддержанием психоэмоционального благополучия. Кроме того, формирование взрослой идентичности усиливает чувствительность к социальному давлению и нормам поведения в онлайн-среде.

*Возрастные особенности и педагогические выводы.* Для старшеклассников ключевым направлением работы является развитие навыков критического мышления, медиа- и информационной грамотности, умения распознавать манипуляции и фейковые источники, а также формирование устойчивости к стрессам, вызванным цифровой средой. Образовательные программы должны уделять особое внимание профилактике интернет-зависимости, управлению цифровым временем, формированию культуры ответственного онлайн-поведения и навыков саморегуляции.

*Методологический вывод.* В старшей школе цифровая грамотность приобретает зрелую форму, но одновременно усиливаются психологические вызовы, связанные с ответственным использованием цифровых ресурсов и социальной самореализацией в сети. Это подтверждает необходимость комплексного сопровождения старшеклассников, которое объединяет техническое обучение, развитие критического мышления и психологическую поддержку, направленную на снижение тревожности и напряженности.

Сравнительный анализ данных (рисунки 1.4.1–1.4.3) позволяет выявить важные возрастные различия и общие тенденции,

характеризующие динамику цифровой грамотности и психологического состояния учащихся в условиях школьной образовательной среды.

*Учащиеся 5–7 классов.* На этом этапе цифровая грамотность только начинает активно формироваться. Школьники осваивают базовые навыки работы с устройствами и программным обеспечением, однако их опыт ограничен, что сопровождается высокой тревожностью и напряженностью при взаимодействии с цифровыми технологиями. Основные источники тревоги связаны с отсутствием опыта, трудностями навигации в цифровой среде и уязвимостью перед базовыми киберугрозами. Таким образом, акцент педагогической работы должен быть сделан на обучении основам безопасного использования цифровых инструментов и формировании позитивного отношения к цифровой среде.

*Учащиеся 8–9 классов.* В среднем звене цифровая грамотность заметно возрастает: подростки свободно пользуются онлайн-сервисами, социальными сетями, цифровыми платформами для обучения и общения. Однако именно в этом возрасте наблюдается рост тревожности и напряженности, обусловленный расширением цифровой активности и столкновением с новыми рисками (кибербуллинг, фишинг, доступ к нежелательному контенту). Знания о возможных угрозах могут усиливать ощущение уязвимости, что подтверждает эффект «осведомленности об опасности». Для этой возрастной группы приоритетом становится формирование критического мышления, медиаграмотности и устойчивости к психологическому давлению в сети.

*Учащиеся 10–11 классов.* В старшей школе цифровая грамотность достигает наиболее высокого уровня: учащиеся уверенно работают с информационными технологиями, понимают правовые и этические нормы цифрового взаимодействия, формируют собственную цифровую идентичность. Однако тревожность сохраняется, приобретая более сложный характер. Теперь она связана не с техническими трудностями, а с социально-психологическими рисками – угрозой репутационных потерь, публичностью в сети, манипуляциями и зависимостью от цифровой среды. Напряженность также остается высокой, но обусловлена сочетанием учебных и социальных факторов: подготовкой к экзаменам, участием в конкурсах, необходимостью балансировать между интенсивным использованием цифровых ресурсов и эмоциональным благополучием.

По мере взросления школьников цифровая грамотность демонстрирует устойчивый рост, однако параллельно наблюдается трансформация тревожности и напряженности. У младших школьников они связаны с нехваткой опыта, у подростков – с ростом цифровой активности и столкновением с новыми угрозами, у

старшеклассников – с социальными и психологическими рисками цифровой идентичности. Это подтверждает необходимость возрастно-дифференцированного подхода к формированию цифровой грамотности: от базового обучения и профилактики у младших школьников к развитию критического мышления и психологической устойчивости у подростков и старшеклассников.

Таким образом, данные трех диаграмм подтверждают, что цифровая грамотность – это не только совокупность технических навыков, но и комплекс социально-психологических характеристик. Ее формирование должно сопровождаться системной педагогической и психологической поддержкой, направленной на снижение тревожности и напряженности в условиях киберопасностей, с учетом возрастных особенностей школьников.

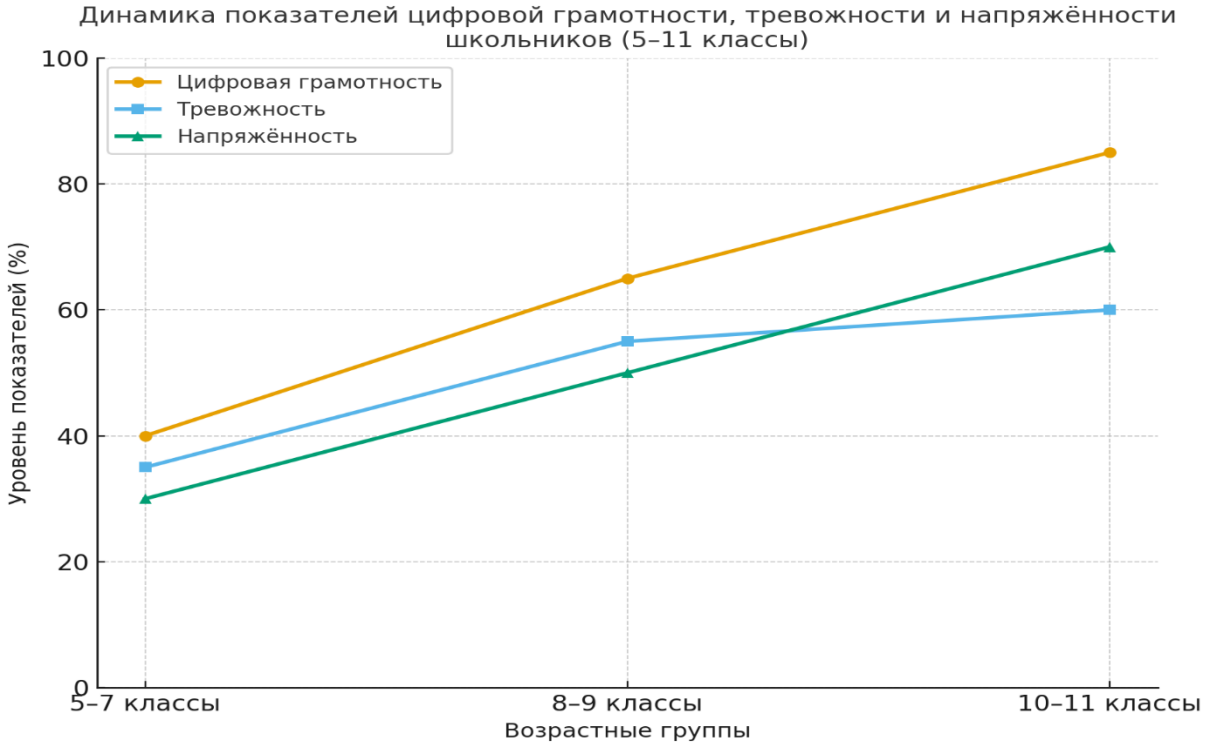



Рисунок 1.4.4 - Сводный график динамики по трем возрастным группам (5–7, 8–9 и 10–11 классы), где отражены показатели цифровой грамотности, тревожности и напряженности

Отраженные на рисунке показатели демонстрируют сравнительную динамику уровня цифровой грамотности, а также степени тревожности и напряженности школьников разных возрастных групп (5–7, 8–9 и 10–11 классы) в контексте воздействия киберопасности.

Анализ графика показывает, что в младшей возрастной группе (5–7 классы) наблюдается наименьший уровень цифровой грамотности. Это объясняется ограниченным опытом взаимодействия

с цифровыми технологиями и отсутствием сформированных навыков критической оценки информации. Вместе с тем именно в этом возрасте тревожность и напряженность имеют довольно высокий показатель, что связано с низкой способностью распознавать и адекватно реагировать на потенциальные угрозы в сети.

В группе 8–9 классов фиксируется заметное повышение уровня цифровой грамотности. Ученики начинают активнее использовать цифровые технологии в учебных и социальных целях, что способствует развитию умений поиска, обработки и безопасного применения информации. Однако именно в этот период возрастает и уровень тревожности: подростки становятся более вовлеченными в интернет-коммуникацию, сталкиваются с явлениями кибербуллинга, риском потери персональных данных, что усиливает их эмоциональное напряжение.

Учащиеся старших классов (10–11) демонстрируют наиболее высокий уровень цифровой грамотности, что проявляется в уверенном владении цифровыми инструментами и навыками критического анализа информации. Благодаря этому тревожность и напряженность снижаются по сравнению с подростковой группой. Старшеклассники более осознанно регулируют свое поведение в цифровой среде, используют знания о киберугрозах и способы защиты, что обеспечивает более устойчивое психоэмоциональное состояние.

Таким образом, сравнительный анализ динамики по возрастам позволяет выделить закономерность: повышение уровня цифровой грамотности сопровождается снижением тревожности и напряженности школьников. Это подчеркивает важность целенаправленного формирования цифровых компетенций начиная с младшего школьного возраста, чтобы минимизировать психологические риски и сформировать устойчивое безопасное поведение в киберпространстве.

Далее представим дополнительно к интерпретации методические рекомендации для педагогов и школьных психологов по каждой возрастной группе:

*5–7 классы*

– Основное направление работы – формирование базовых навыков безопасного поведения в сети.

– Необходимо в игровой форме обучать правилам пользования интернетом: что можно публиковать, как реагировать на незнакомцев, как отличать «дружественные» и «опасные» ситуации.

– Важно развивать навыки эмоциональной саморегуляции и снижать тревожность через интерактивные занятия, обсуждение реальных, но адаптированных для возраста примеров.

– Полезны совместные родительско-ученические проекты по кибербезопасности, чтобы формировать единое информационное пространство доверия.

*8–9 классы*

- В этом возрасте важно акцентировать внимание на рисках цифровой среды: кибербуллинг, фишинг, мошенничество.
- Следует организовывать тренинги по развитию критического мышления и цифровой медиаграмотности (например, как отличить фейковую информацию, проверить источник).
- Необходимо внедрять групповые обсуждения и кейс-методы для проработки типичных проблемных ситуаций (например, «Что делать, если украли аккаунт?»).
- В психологической работе следует акцентировать внимание на навыках стрессоустойчивости и конструктивного взаимодействия в онлайн-среде.

*10–11 классы*

- У старшеклассников акцент смещается на развитие цифровой ответственности и самоконтроля.
- Рекомендуется внедрять проектные задания: создание собственных медиапродуктов, разработка «школьных правил киберэтикета», участие в киберволонтерстве.
- Полезны мастер-классы по углубленным вопросам кибербезопасности (защита персональных данных, работа с цифровыми следами, основы киберэтики).
- В психологическом сопровождении важно формировать у подростков чувство уверенности в себе и своей способности контролировать собственное поведение в сети.

Таким образом, педагогическая и психологическая работа должна быть *возрасто-дифференцированной*: от элементарных правил и игровой профилактики (5–7 кл.) через развитие критического мышления и навыков анализа рисков (8–9 кл.) до формирования ответственного и осознанного цифрового поведения (10–11 кл.).

Отдельно мы выделяем оценку степени цифровой тревожности, которая проводилась по критериям 5-ти компонентов (таблица 1.4.3).

Таблица 1.4.3 – Критерии цифровой тревожности (КЦТ)

1. Когнитивный компонент (осознанные установки и страхи)

| Подкритерий | Что оценивает |
|---|---|
| Страх утечки личных данных | Тревожность при использовании логинов, паролей, форм с персональными данными. |
| Недоверие к цифровой информации | Склонность видеть в цифровом пространстве угрозу, манипуляцию, фейки. |
| Страх перед цифровыми ошибками | Боязнь случайно удалить, опубликовать, не так интерпретировать информацию. |

2. Эмоциональный компонент

| Подкритерий | Что оценивает |
|---|---|
| Чувство | Состояние фрустрации при сбоях, вирусах, |

| | |
|---|---|
| беспомощности в сети | технических ошибках. |
| Нарастающее беспокойство при онлайн-активности | Эмоциональная неуверенность, стресс, навязчивые мысли. |
| Страх оценки/осуждения | Боязнь быть высмеянным, публично осужденным, «отмененным» в интернете. |

3. Поведенческий компонент

| Подкритерий | Что оценивает |
|---|---|
| Избегающее поведение | Намеренное ограничение участия в онлайн-активностях (например, отказ от видеозвонков, соцсетей). |
| Зависимое поведение | Проверка уведомлений, лайков, сообщений с целью снятия тревоги. |
| Импульсивность в сети | Поспешная публикация, удаление сообщений, реакция «на эмоциях». |

4. Социальный компонент

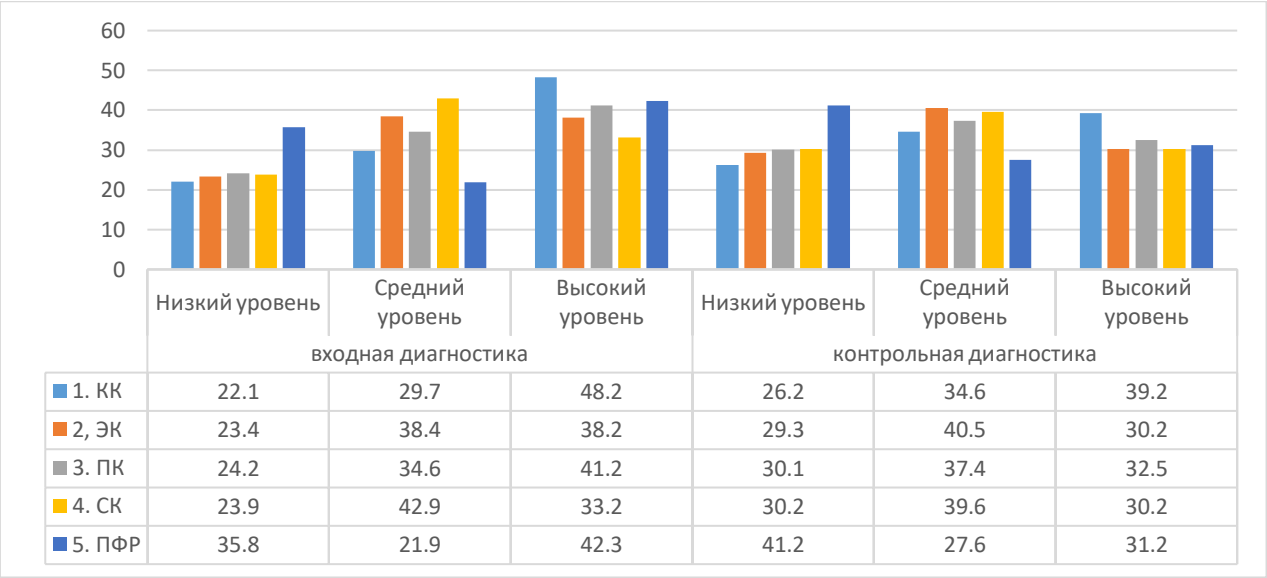
| Подкритерий | Что оценивает |
|---|---|
| Страх кибербуллинга | Ожидание или опыт цифровой агрессии со стороны сверстников/коллег. |
| Недоверие к онлайн-коммуникации | Сложности с построением доверительных отношений в мессенджерах и соцсетях. |
| Цифровая изоляция | Ощущение одиночества, отчуждения, несмотря на постоянную «онлайн-связь». |

5. Психофизиологические реакции

| Подкритерий | Что оценивает |
|---|---|
| Соматические проявления при взаимодействии с ИКТ | Головные боли, утомляемость, тревожное дыхание во время работы за экраном. |
| Нарушения сна, связанные с онлайном | Просмотр сообщений ночью, страх пропустить важное, нарушения режима. |

Возможные уровни цифровой тревожности:

- Низкий (6–12 баллов): комфортное цифровое поведение;
- Средний (13–20 баллов): периодическое беспокойство, нуждается в профилактике;
- Высокий (21+ баллов): выраженная цифровая тревожность, рекомендуется коррекционная работа.




| | Низкий уровень | Средний уровень | Высокий уровень | Низкий уровень | Средний уровень | Высокий уровень |
|---|---|---|---|---|---|---|
| | входная диагностика | | | контрольная диагностика | | |
| 1. КК | 22.1 | 29.7 | 48.2 | 26.2 | 34.6 | 39.2 |
| 2, ЭК | 23.4 | 38.4 | 38.2 | 29.3 | 40.5 | 30.2 |
| 3. ПК | 24.2 | 34.6 | 41.2 | 30.1 | 37.4 | 32.5 |
| 4. СК | 23.9 | 42.9 | 33.2 | 30.2 | 39.6 | 30.2 |
| 5. ПФР | 35.8 | 21.9 | 42.3 | 41.2 | 27.6 | 31.2 |

Рисунок 1.4.5 – Показатели динамики цифровой тревожности: 5-7 классы (в%)

В младших подростков цифровая тревожность проявляется в первую очередь как страх столкнуться с непонятными или опасными ситуациями в интернете (незнакомые люди, вирусы, потеря доступа к аккаунту). Данные диаграммы показывают, что тревожность здесь имеет неравномерный характер: часть учеников испытывает высокий уровень напряженности, другая часть – практически не тревожится, так как еще не вовлечена глубоко в цифровую среду.

Выводы:

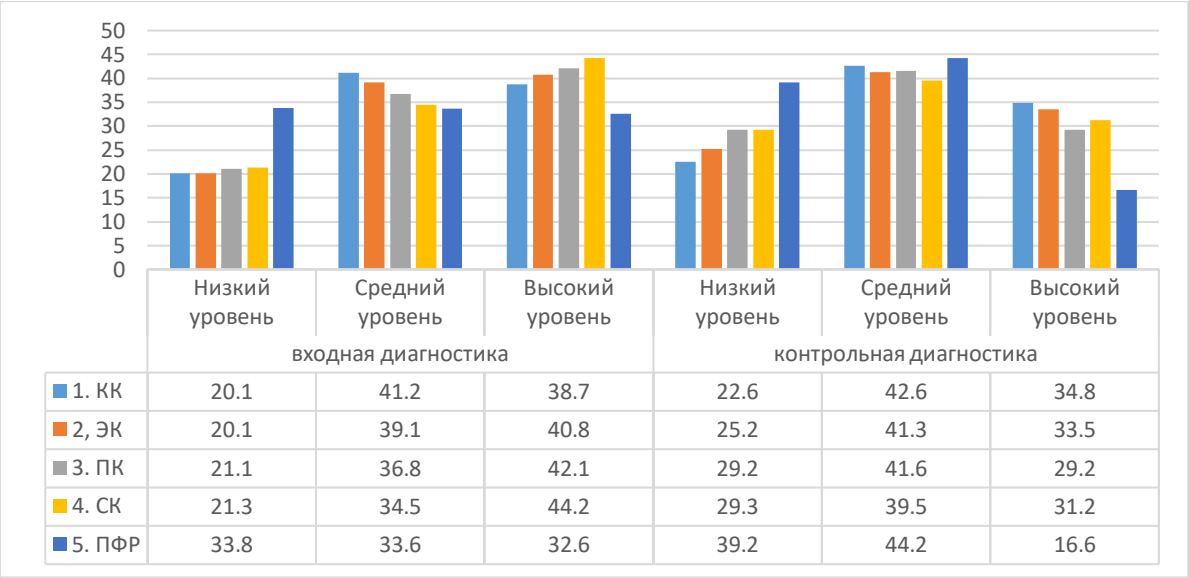
– Неустойчивость показателей связана с отсутствием опыта и знаний: школьники этого возраста часто не понимают, что именно может быть опасно.

– Формируется начальная зависимость от гаджетов, но еще без выраженных признаков цифрового стресса.

– Рекомендации:

– Педагогу: обучать базовым правилам безопасного пользования цифровыми устройствами, акцентировать внимание на позитивных сценариях использования.

– Психологу: снижать избыточную тревожность через игровые формы, беседы о «страшных» интернет-мифах, формирование доверительных отношений.




| | Низкий уровень | Средний уровень | Высокий уровень | Низкий уровень | Средний уровень | Высокий уровень |
|---|---|---|---|---|---|---|
| | входная диагностика | | | контрольная диагностика | | |
| 1. КК | 20.1 | 41.2 | 38.7 | 22.6 | 42.6 | 34.8 |
| 2, ЭК | 20.1 | 39.1 | 40.8 | 25.2 | 41.3 | 33.5 |
| 3. ПК | 21.1 | 36.8 | 42.1 | 29.2 | 41.6 | 29.2 |
| 4. СК | 21.3 | 34.5 | 44.2 | 29.3 | 39.5 | 31.2 |
| 5. ПФР | 33.8 | 33.6 | 32.6 | 39.2 | 44.2 | 16.6 |

Рисунок 1.4.6 – Показатели динамики цифровой тревожности: 8-9 классы (в%)

В среднем звене тревожность значительно возрастает. Школьники начинают активно использовать соцсети, участвовать в онлайн-играх и сталкиваться с рисками: кибербуллингом, давлением со стороны сверстников, страхом «выпасть из сети» (FOMO). Данные диаграммы показывают рост числа учащихся с выраженным уровнем цифровой тревожности по сравнению с младшими классами.

Выводы:

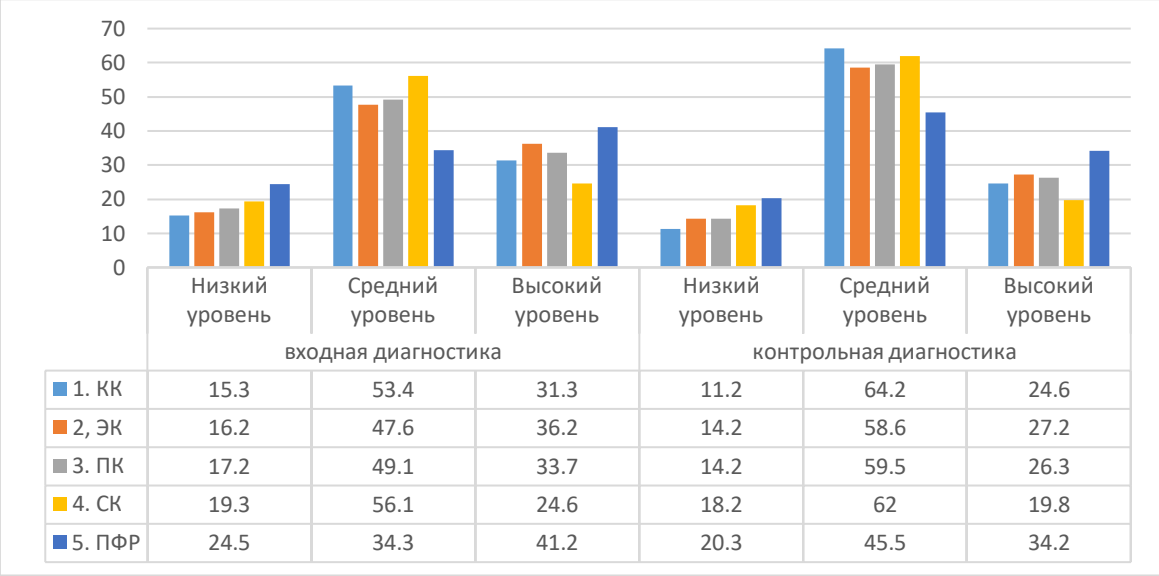
– Основная причина – усиление социальной зависимости от цифровой среды и активное взаимодействие с ней.

– В этот период возникает потребность в умении управлять своими эмоциями при столкновении с онлайн-рисками.

– Рекомендации:

– Педагогу: внедрять тренинги по цифровой гигиене, обсуждать реальные примеры киберугроз и способы их преодоления.

– Психологу: развивать навыки стрессоустойчивости, формировать культуру общения в сети, обучать приемам преодоления буллинга и социальной тревожности.




| | Низкий уровень | Средний уровень | Высокий уровень | Низкий уровень | Средний уровень | Высокий уровень |
|---|---|---|---|---|---|---|
| | входная диагностика | | | контрольная диагностика | | |
| 1. КК | 15.3 | 53.4 | 31.3 | 11.2 | 64.2 | 24.6 |
| 2, ЭК | 16.2 | 47.6 | 36.2 | 14.2 | 58.6 | 27.2 |
| 3. ПК | 17.2 | 49.1 | 33.7 | 14.2 | 59.5 | 26.3 |
| 4. СК | 19.3 | 56.1 | 24.6 | 18.2 | 62 | 19.8 |
| 5. ПФР | 24.5 | 34.3 | 41.2 | 20.3 | 45.5 | 34.2 |

Рисунок 1.4.7 – Показатели динамики цифровой тревожности: 10-11 классы (в%)

У старшеклассников наблюдается *снижение уровня тревожности* по сравнению с 8–9 классами. Это объясняется большей зрелостью, опытом использования цифровых технологий и формированием базовых защитных стратегий. Однако часть подростков продолжает испытывать тревожность из-за страха потерять контроль над своей цифровой идентичностью (утечка данных, «цифровой след», давление со стороны сверстников).

Выводы:

– Старшеклассники лучше адаптированы к рискам, но их тревожность носит более осознанный характер (не «неизвестно чего боюсь», а конкретные страхи: утечки данных, блокировки аккаунта, оценка со стороны других).

– Уровень тревожности здесь связан с саморефлексией и подготовкой к будущей взрослой жизни.

Рекомендации:

– Педагогу: организовывать проектные задания (создание «цифрового портфолио», разработка правил сетевого этикета).

– Психологу: работать над укреплением уверенности в себе, развивать навыки ответственного использования цифровых ресурсов, помогать в формировании личных стратегий самозащиты в сети.

В целом динамика такова:

– 5–7 классы – тревожность ситуативна, связана с неизвестностью.

– 8–9 классы – тревожность на пике из-за социальной вовлеченности и давления среды.

– 10–11 классы – тревожность снижается, становится более рациональной и избирательной.

Ниже представлена сравнительная таблица по результатам анализа трех диаграмм (рисунки 1.4.5–1.4.7).

Таблица 1.4.4 – Сравнительная таблица динамики цифровой тревожности у школьников

| Возрастная группа | Основные причины цифровой тревожности | Особенности проявления | Педагогические стратегии | Психологические стратегии |
|---|---|---|---|---|
| 5–7 классы | • Недостаток знаний о цифровых рисках<br>• Столкновение с «неизвестностью» в интернете<br>• Первичное формирование зависимости от гаджетов | • Неравномерный характер (у одних высокая тревожность, у других почти отсутствует)<br>• Страх перед «мифическими» угрозами | • Обучение базовым правилам цифровой гигиены<br>• Использование игровых форм и примеров из жизни | • Снижение избыточной тревожности через игры и беседы<br>• Формирование доверия к взрослым как к помощникам |
| 8–9 классы | -Активное использование соцсетей и игр<br>-Кибербуллинг, FOMO («страх упустить»)<br>-Давление со стороны сверстников | -Наибольший уровень цифровой тревожности<br>-Зависимость от оценок и реакций онлайн-среды | • Внедрение тренингов по цифровой гигиене<br>• Обсуждение реальных случаев киберугроз и способов их предотвращения | • Развитие стрессоустойчивости<br>• Обучение навыкам преодоления буллинга<br>• Формирование культуры сетевого общения |
| 10–11 классы | • Осознанные страхи (утечка данных, цифровой след)<br>• Опасения за репутацию и будущее<br>• Стремление контролировать цифровую идентичность | • Снижение тревожности по сравнению с 8–9 классами<br>• Тревожность более рациональная, избирательная | • Организация проектных заданий (цифровое портфолио, правила сетевого этикета)<br>• Обучение ответственному использованию технологий | • Укрепление уверенности в себе<br>• Помощь в формировании личных стратегий защиты в сети<br>• Поддержка в саморефлексии и планировании будущего |

Таким образом, цифровая тревожность у школьников имеет ярко выраженную возрастную динамику: от неопределенных страхов у младших подростков к пику социальной тревожности в среднем звене и к более рациональному, осознанному характеру у старшеклассников.

# ГЛАВА 2. КОМПЛАЕНС-МЕНЕДЖМЕНТ В СФЕРЕ ОБРАЗОВАНИЯ

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

В условиях активной цифровизации системы школьного образования вопросы информационной безопасности и защиты персональных данных приобретают стратегическое значение. Широкое внедрение электронных журналов, систем дистанционного обучения, облачных сервисов и мобильных приложений формирует новые возможности для обучения, однако одновременно усиливает уязвимости школьных экосистем перед киберугрозами. Растущее количество атак на образовательные учреждения, случаи утечек данных и неправомерного использования информации о детях подчеркивают необходимость построения комплексных систем комплаенс-менеджмента и управления рисками кибербезопасности. Правительства, предприятия и школы стали жертвами кибератак, киберпреступлений и киберсбоев. Несмотря на повышенное внимание и возросший уровень инвестиций в кибербезопасность, количество киберинцидентов, связанные с ними затраты и их влияние на здоровье людей, продолжает расти [81].

В первые годы активного внедрения цифровых технологий вопросы, связанные с человеческим фактором, практически не изучались и долгое время оставались в тени. Однако рост числа кибератак, утечек персональных данных и случаев использования программ-вымогателей показал, что именно ошибки пользователей часто становятся ключевой причиной инцидентов. По данным исследований, до 95% всех происшествий в сфере кибербезопасности так или иначе связаны с человеческим участием [82]. Современная кибербезопасность представляет собой сложное взаимодействие автоматизированных систем и человека, что делает уязвимыми как цифровые технологии, так и пользователей.

Результаты многочисленных исследований подтверждают, что недостаточный уровень цифровой компетентности и низкая осведомлённость сотрудников в вопросах безопасности остаются основными факторами риска [83]. Несмотря на развитие инструментов и технологий защиты, именно человек остаётся центральным элементом в обеспечении киберустойчивости организации. Первичный анализ состояния цифровой среды в школах также выявил недостаточную информированность участников образовательного процесса в области киберзащиты, кибербезопасности и киберэтики [84].

Осенью 2022 года в казахстанском сегменте интернета (Казнет) было зафиксировано резкое увеличение числа кибератак — их интенсивность возросла в сотни раз. Наблюдались масштабные целенаправленные атаки на различные сетевые ресурсы, что наглядно продемонстрировало их уязвимость и подчеркнуло необходимость усиления мер защиты цифровой образовательной среды. Особую актуальность данная проблема приобретает в школьном секторе, поскольку образовательные организации активно используют информационные системы и онлайн-платформы, такие как Kundelik.kz, Bilimland.kz, Ekitap.kz и Onlinemektep.kz.

Участившиеся инциденты, связанные с киберугрозами, выявили наличие в школьной среде ряда проблем, требующих системного решения. Среди них — недостаточная осведомлённость участников образовательного процесса в вопросах киберэтики, учащиеся сталкиваются с кибербуллингом, нарушением конфиденциальности персональных данных и угрозами вирусных атак. Кроме того, зафиксированы случаи неправомерной передачи логинов и паролей, несанкционированного доступа к электронным журналам и попыток повторного изменения оценок, что свидетельствует о необходимости усиления цифровой грамотности, киберзащиты и формирования культуры ответственного поведения в онлайн-пространстве.

Одним из ключевых инструментов обеспечения требований кибербезопасности в образовательных организациях является комплаенс-менеджмент, который направлен на приведение внутренних процессов, регламентов и технологий в соответствие с установленными стандартами и нормативами. В школьной среде этот подход играет особую роль, поскольку именно здесь обрабатывается значительный объем персональных данных учащихся, родителей и педагогов, а также осуществляется активное использование цифровых образовательных платформ и информационных систем.

В Казахстане комплаенс-менеджмент является относительно новым явлением, особенно в контексте школьного образования, где процедуры системного управления соответствием пока находятся на этапе формирования и внедрения. Большинство школ ограничиваются техническими мерами защиты, при этом комплексные стратегии управления рисками кибербезопасности и интегрированные комплаенс-программы еще только начинают разрабатываться. Отсутствие единых стандартов и недостаточная методическая поддержка образовательных учреждений создают необходимость более глубокого научного изучения проблем и перспектив внедрения комплаенс-менеджмента в данной сфере.

В рамках настоящего теоретического обзора были сформулированы исследовательские вопросы, направленные на систематизацию существующих подходов и выявление направлений дальнейших исследований: Какие риски кибербезопасности

характерны для современной школьной среды? Какие механизмы и практики комплаенс-менеджмента в области кибербезопасности применяются в образовательных учреждениях, и насколько они адаптированы к условиям школьного сектора?

Ответы на эти вопросы позволят не только обобщить мировой и отечественный опыт, но и определить наиболее эффективные модели и инструменты внедрения комплаенс-менеджмента в школах Казахстана, учитывая их специфику и ресурсные возможности.

Для поиска ответов на поставленные исследовательские вопросы был применён метод теоретического обзора научных исследований с использованием базы данных Google Scholar. В анализ включались публикации за период с 2019 по 2022 годы, что позволило сосредоточиться на наиболее актуальных подходах и современных практиках в области кибербезопасности школьной среды.

Процесс теоретического обзора проводился в несколько последовательных этапов, включающих: формулирование исследовательских вопросов и постановку цели поиска; разработку стратегии поиска релевантных источников; определение критериев отбора публикаций; проведение анализа и интерпретации данных; синтез полученной информации для выявления ключевых закономерностей и выводов [5; 4].

В качестве основного поискового запроса была использована комбинация ключевых слов: "school cybersecurity" AND compliance. По результатам поиска было обнаружено 28 публикаций, из которых семь были отобраны для дальнейшего анализа на основе заранее определённых критериев. В выборку включались только работы, написанные на английском языке, содержащие эмпирические или теоретические материалы, непосредственно относящиеся к обеспечению соответствия требованиям кибербезопасности в школьной среде.

Из анализа были исключены исследования, сосредоточенные исключительно на подготовке специалистов или преподавании кибербезопасности в образовательных учреждениях, поскольку их содержание не соответствовало целям настоящего обзора. В следующем разделе представлен качественный и количественный анализ выбранных исследований, что позволило оценить существующие практики и подходы к управлению рисками и комплаенс-менеджменту в школьной среде. Важно подчеркнуть, что количество публикаций по данной теме остаётся ограниченным, что свидетельствует о недостаточной разработанности проблематики комплаенс-менеджмента кибербезопасности в системе школьного образования и указывает на необходимость дальнейших исследований в этой области.

Для ответа на первый исследовательский вопрос — «Какие риски кибербезопасности характерны для школьной среды?» — был

проведён углублённый анализ отобранных публикаций, направленный на выявление и систематизацию факторов, влияющих на защищённость цифровой образовательной инфраструктуры. Полученные результаты показали, что сфера образования относится к числу наиболее уязвимых секторов в области кибербезопасности, что подтверждается данными ряда международных исследований. Согласно отчётам аналитических компаний и научных публикаций, сектор образования в 2018 году был признан одним из наименее защищённых среди всех сфер деятельности, демонстрируя наибольшее количество выявленных уязвимостей и зафиксированных киберинцидентов [86].

Ситуация существенно осложнилась в период массового внедрения дистанционного обучения, что стало особенно заметно в 2020 году, когда школы по всему миру перешли на онлайн-форматы. По данным исследователей, именно в этот период наблюдался рекордный рост количества публично зарегистрированных инцидентов кибербезопасности в образовательных организациях. Массовое использование облачных платформ, онлайн-дневников, видеоконференций и электронных журналов увеличило количество атак на школьные информационные системы, что существенно повысило их уязвимость [87].

В анализируемых исследованиях приводятся различные примеры кибератак на школьные ресурсы за последние пять лет. Наиболее распространёнными угрозами являются:

– фишинг - рассылка вредоносных сообщений, направленных на получение логинов и паролей;

– распределённые атаки типа «отказ в обслуживании» (DDoS), приводящие к временной недоступности образовательных платформ;

– атаки с компрометацией деловой электронной почты (BEC-атаки), направленные на подмену финансовых реквизитов или получение конфиденциальной информации;

– атаки программ-вымогателей (ransomware), блокирующие доступ к цифровым ресурсам школы и требующие выкуп за их восстановление;

– социальная инженерия — целенаправленные манипуляции учащимися и педагогами для получения конфиденциальных данных.

Особое внимание уделяется исследованию Torres, Mullins и Thompson, в котором подчёркивается, что недостаток ресурсов, ограниченное внимание к вопросам киберзащиты и низкий уровень осведомлённости делают школы лёгкой целью для злоумышленников. Авторы отмечают, что образовательные учреждения зачастую медленно реагируют на киберинциденты и не обладают необходимыми знаниями и инфраструктурой для эффективного устранения угроз [84]. В отчётах также зафиксирован рост числа атак

с использованием программ-вымогателей, а в качестве решения предлагаются разработка технических планов реагирования и повышение готовности школ к инцидентам.

Кроме того, значительная часть угроз связана с человеческим фактором. Исследования показывают, что ошибки пользователей, недостаточная подготовка педагогов и сотрудников школ, слабое восприятие киберугроз, несоблюдение правил кибербезопасности и неэффективная организационная культура являются важными факторами риска [87]. В совокупности эти проблемы усиливают уязвимость образовательных учреждений и подчеркивают необходимость развития комплексных стратегий по управлению киберрисками и формированию культуры цифровой безопасности.

Согласно исследованию M. Richardson и соавторов, к числу ключевых типов киберсобытий, оказывающих значительное влияние на уровень кибербезопасности в школьной среде, относятся несколько категорий рисков. Во-первых, это технические угрозы, связанные с уязвимостями инфраструктуры и недостаточной защищённостью систем информационной безопасности образовательных учреждений. Во-вторых, особое внимание уделяется рискам утечки персональных данных, которые возникают как в результате внешних атак, так и вследствие недостаточной цифровой грамотности пользователей. Кроме того, выделяются угрозы, связанные с доступом к незаконному или неподобающему контенту, а также различные формы онлайн-агрессии - киберзапугивание, киберпреследование и цифровые домогательства. Отдельно подчеркивается риск непреднамеренного раскрытия конфиденциальной информации учащимися, например, при фишинговых атаках или при обмене личными данными в социальных сетях и на открытых онлайн-платформах [88].

Публикации последних лет фиксируют значительное расширение спектра угроз, с которыми сталкиваются школы. Среди наиболее распространённых инцидентов в образовательной системе отмечаются: мошенничество с использованием платежных карт, несанкционированный доступ к конфиденциальной информации, взлом школьных аккаунтов и внедрение вредоносного программного обеспечения, потеря или уничтожение данных, инсайдерские угрозы, порча веб-сайтов и страниц в социальных сетях, а также вторжения в онлайн-классы и виртуальные собрания (например, во время проведения дистанционных уроков) [89], [90].

Помимо технических аспектов, значительное внимание уделяется психосоциальным рискам, которые формируются внутри школьной цифровой среды. Исследователи подчёркивают необходимость учитывать такие явления, как кибербуллинг, навязчивое вовлечение в интернет-игры, рискованное поведение в онлайн-пространстве, кибер-агрессия и распространение кибер-сплетен, поскольку они напрямую влияют не только на безопасность данных, но и на психологическое

здоровье учащихся, а также на климат внутри школьного сообщества [91].

Таким образом, анализ литературы подтверждает, что риски кибербезопасности в школьной среде имеют комплексный характер, охватывая как технические, так и социально-психологические аспекты. Угрозы, связанные с уязвимостью информационных систем, тесно переплетаются с проблемами цифровой культуры и безопасного поведения пользователей. Это указывает на необходимость системного подхода к разработке и внедрению школьных стратегий киберзащиты, включающих не только совершенствование технической инфраструктуры, но и формирование цифровой грамотности, культуры киберэтики и ответственного онлайн-поведения у всех участников образовательного процесса. В таблице 1.4.1 представлен обобщенный список рисков, рассмотренных в анализируемых исследованиях.

Таблица 1.4.1 Риски кибербезопасности в системе школьного образования

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

Для ответа на второй исследовательский вопрос — «Какие механизмы комплаенс-менеджмента системы школьного образования в области кибербезопасности применяются в школах?» - был проведён анализ отобранных исследований, направленный на выявление мер и практик, обеспечивающих соблюдение требований киберзащиты и защиты данных в образовательной среде.

Результаты обзора показывают, что важнейшей задачей образовательных учреждений является внедрение комплексных механизмов комплаенс-менеджмента, которые позволяют обеспечить соответствие процессов обработки данных требованиям национального законодательства, международных стандартов и внутренних регламентов. Исследователи E. Belastock и M. Torres подчёркивают, что одним из ключевых инструментов в данном направлении является разработка и соблюдение политики кибербезопасности, которая должна иметь системный и многоуровневый характер [86].

В рамках реализации таких политик выделяются несколько основных направлений деятельности. Прежде всего, особое внимание уделяется повышению уровня цифровой грамотности и осведомлённости всех участников образовательного процесса - педагогов, учащихся, родителей и сотрудников администрации. Школы внедряют программы по обучению основам киберэтики, безопасного поведения в сети и методам защиты персональных данных.

Следующим важным механизмом является разработка и внедрение нормативных актов и регламентов по кибербезопасности, включая правила хранения и передачи информации, порядок предоставления доступа к образовательным платформам и облачным сервисам, а также определение ответственности за соблюдение установленных требований.

Не менее значимыми направлениями являются:

- регулирование доступа цифровых устройств к школьным ресурсам, что предполагает создание многоуровневых систем аутентификации и разграничение прав пользователей;
- фильтрация входящей электронной корреспонденции и предотвращение фишинговых атак посредством использования специализированных шлюзов безопасности;
- своевременное обновление антивирусных решений и внедрение централизованных систем управления киберзащитой для мониторинга состояния инфраструктуры и выявления уязвимостей в режиме реального времени [86].

Анализ литературы показывает, что одной из наиболее серьёзных угроз для школ является риск утечки или кражи персональных данных, поскольку образовательные учреждения обрабатывают и хранят большой объём конфиденциальной информации. К таким

данным относятся сведения об учащихся, их родителях, выпускниках, преподавателях и сотрудниках школ. Особенность заключается в том, что эти записи сохраняются длительное время — иногда десятилетиями после окончания обучения, что делает образовательные учреждения особенно привлекательными объектами для киберпреступников.

Дополнительную сложность создаёт децентрализованная структура хранения данных, характерная для большинства школ. В условиях отсутствия единой централизованной системы обеспечения кибербезопасности сведения могут храниться в разных местах: часть — на локальных серверах отдельных школ, часть - в районных или городских образовательных управлениях, а финансовая информация - на отдельных специализированных ресурсах. Такая разрозненность создаёт дополнительные уязвимости и предоставляет злоумышленникам больше возможностей для компрометации систем, поскольку защита в отдельных сегментах образовательной инфраструктуры часто реализована на разном уровне.

В этом контексте комплаенс-менеджмент предполагает не только внедрение технических мер, но и формирование единой стратегии управления киберрисками. Это включает проведение регулярных аудитов безопасности, оценку уязвимостей, разработку планов реагирования на инциденты и создание единых стандартов защиты данных на всех уровнях школьной системы. Подобный подход позволяет минимизировать риски и обеспечить соблюдение нормативных требований, одновременно формируя культуру ответственного отношения к цифровой информации.

Комплаенс-менеджмент в системе школьного образования основывается на разработке и реализации плана кибербезопасности, который направлен на создание единой стратегии защиты данных и информационных ресурсов школы. Такой план включает несколько ключевых направлений: обучение сотрудников и учащихся основам цифровой безопасности, формирование доверия к процедурам киберзащиты и разработку комплексной политики обеспечения информационной безопасности [88].

Политика кибербезопасности является центральным элементом комплаенс-менеджмента и представляет собой набор обязательных руководящих принципов, определяющих правила безопасного поведения при использовании цифровых систем и работе с персональными данными. Эти документы разрабатываются с учётом миссии, целей и ценностей образовательной организации и служат основой для выстраивания культуры информационной безопасности в школе. Политика направлена на обмен протоколами безопасности, установление чётких ролей и обязанностей сотрудников, а также предоставление инструкций и рекомендаций, которые помогают всем

участникам образовательного процесса обеспечивать защиту данных в повседневной деятельности.

Важным аспектом политики является также регламентация действий в случае инцидентов информационной безопасности. Чётко прописанные роли и обязанности позволяют сотрудникам и учащимся понимать, к кому необходимо обращаться, как фиксировать проблему и какие шаги предпринимать для устранения последствий угрозы. Такой подход повышает уровень готовности образовательного учреждения к возможным киберинцидентам и способствует снижению рисков.

Некоторые исследователи отмечают необходимость создания непрерывных программ обеспечения информационной безопасности, которые должны носить системный характер и включать регулярное обновление мер защиты, проведение тренингов и совершенствование внутренних стандартов [88], [89]. Среди приоритетных направлений выделяется разработка адаптированных стандартов кибербезопасности для школьных образовательных систем, включающих специализированные инструменты самооценки уровня защищенности [90]. Такие инструменты позволяют школам проводить регулярный аудит своих информационных систем, выявлять уязвимости и своевременно разрабатывать корректирующие меры.

Одним из ключевых направлений является предотвращение киберрисков среди учащихся, что требует стратегического и комплексного подхода. Современные исследования подчеркивают необходимость формирования у школьников эмоциональной компетентности и навыков ответственного поведения в сети. Это помогает снизить риски, связанные с кибервиктимизацией, кибербуллингом, распространением кибер-сплетен и другими формами онлайн-агрессии. Ученики должны быть информированы о том, как правильно управлять своей конфиденциальностью при обмене личными данными, а также о возможных угрозах, возникающих при неосмотрительном поведении в социальных сетях и мессенджерах [91].

Особую роль играет родительское сопровождение, которое должно быть интегрировано в план действий школы по защите учащихся от киберугроз. Вовлечение родителей в процесс формирования безопасного цифрового поведения позволяет повысить эффективность профилактических мер и обеспечить комплексный подход к защите детей в онлайн-пространстве.

Таким образом, предотвращение киберрисков в школьной среде должно строиться на основе комплексной, продуманной и устойчивой стратегии, включающей технические, организационные, правовые и педагогические механизмы. Целью таких программ является создание безопасной образовательной цифровой среды, в которой учащиеся могут использовать интернет и цифровые ресурсы с минимальными

угрозами для своих данных, психологического состояния и личной информации.

На основании проведённого теоретического обзора научных исследований были определены основные механизмы комплаенс-менеджмента в системе школьного образования в области кибербезопасности. Подробный анализ этих механизмов представлен в таблице 2.1.2.

Таблица 2.2.2 - Механизмы комплаенс-менеджмента

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

Определение рисков кибербезопасности и анализ механизмов комплаенс-менеджмента в школьной среде создают основу для оценки состояния системы киберзащиты образовательных учреждений и способствуют разработке и внедрению эффективной политики комплаенс-контроля в системе школьного образования Республики Казахстан.

В настоящее время информационная безопасность в Казахстане регулируется государственной концепцией «Киберщит Казахстана», которая определяет основные меры по защите национального киберпространства и инфраструктуры. Однако данный документ носит преимущественно стратегический характер и не содержит конкретных процедур, направленных на обеспечение соответствия образовательных организаций требованиям информационной безопасности и стандартам киберзащиты. В рамках государственной политики утверждены единые требования в области ИКТ и информационной безопасности, включающие методики оценки рисков, правила классификации и маркировки информационных активов, процедуры инвентаризации и паспортизации вычислительной техники, а также нормативные документы для банковской и страховой сферы [92]. Несмотря на это, существующие

регламенты и процедуры не адаптированы для применения в школьной среде и не учитывают специфику образовательного процесса.

Школы являются активными генераторами и хранителями больших объёмов данных, связанных с учебным процессом, административным управлением, кадровым обеспечением и организацией учебных планов. Эти сведения включают персональные данные учащихся, родителей, педагогов и сотрудников школ. Однако значительная часть данных обрабатывается с использованием онлайн-сервисов и платформ сторонних разработчиков, которые не всегда соответствуют требованиям национальных стандартов кибербезопасности. В большинстве случаев предполагаемые риски использования сторонних интернет-ресурсов не оцениваются, а политики безопасности не охватывают их в полном объёме.

Кроме того, существует недостаточная осведомлённость педагогов и учащихся о современных киберугрозах. Исследования показывают, что как школьники, так и сотрудники школ часто не обладают необходимыми знаниями для оценки опасности использования онлайн-сервисов, а педагоги нередко не готовы интегрировать обучение цифровой безопасности в образовательный процесс [89], [86]. Эта ситуация создаёт дополнительные уязвимости и повышает вероятность утечек данных, несанкционированного доступа к цифровым платформам и нарушений конфиденциальности.

В сложившихся условиях для казахстанских школ необходима разработка единых стандартов цифровой безопасности, включающих:

- создание нормативно-правовой базы, адаптированной к особенностям образовательного процесса;
- разработку политики информационной безопасности на уровне школ и районных управлений;
- подготовку методических рекомендаций для педагогов и сотрудников ИКТ-подразделений;
- внедрение инструментов оценки и мониторинга киберрисков.

Особую роль в этом процессе играет комплаенс-менеджмент, который обеспечивает согласование внутренней нормативно-правовой документации образовательных организаций с национальными стандартами и международными требованиями в сфере кибербезопасности [82]. Использование комплексного подхода к комплаенс-менеджменту позволяет внедрять единые процедуры контроля, применять современные инструменты мониторинга и разрабатывать методические руководства для педагогов и администрации школ [83].

На основе анализа современных научных источников и международного опыта был сформирован алгоритм комплаенс-менеджмента по обеспечению кибербезопасности в школьной среде [81], [82]. Этот алгоритм представляет собой системную модель,

включающую оценку рисков, разработку политики безопасности, распределение ответственности, внедрение технических и организационных мер, а также регулярный мониторинг и совершенствование системы.

Проведенный теоретический обзор исследований позволил выявить комплекс рисков кибербезопасности, характерных для школьной среды, которые необходимо учитывать при разработке и внедрении комплаенс-менеджмента в системе обеспечения информационной безопасности образовательных организаций. Настоящее исследование направлено на определение необходимости формирования целостной системы комплаенс-управления кибербезопасностью в школах через выявление потенциальных угроз и факторов уязвимости, возникающих в условиях активного включения образовательных учреждений в цифровое пространство.

Вовлечение школ в глобальное киберпространство сопровождается не только расширением образовательных возможностей, но и повышением интереса злоумышленников к цифровым ресурсам и персональным данным учащихся, педагогов и сотрудников администрации. Особую значимость приобретают проблемы, связанные с недостаточным уровнем цифровой грамотности и низкой осведомленностью участников образовательного процесса о киберугрозах. Ошибки сотрудников, педагогов и самих учащихся, связанные с использованием информационных систем, значительно повышают вероятность возникновения инцидентов и создают дополнительные уязвимости для школьной киберсреды.

Результаты анализа литературы позволили систематизировать основные риски кибербезопасности, с которыми наиболее часто сталкиваются школы. Среди них выделяются:

- социальная инженерия и методы психологического воздействия на пользователей;
- фишинг и скимминг с целью получения данных учётных записей;
- угрозы, связанные с технологической уязвимостью информационных систем и оборудования;
- утечка или потеря данных вследствие недостаточной защиты хранилищ и облачных сервисов;
- нарушения конфиденциальности персональной и учебной информации;
- киберзапугивание, киберпреследование и другие формы киберагрессии;
- инсайдерские угрозы - неправомерные действия сотрудников или учащихся;
- мошенничество и компрометация систем с целью получения доступа к учебным или финансовым данным;

- захват учётных записей и аккаунтов в электронных журналах и образовательных платформах;

- вторжения в онлайн-классы и виртуальные школьные собрания;

- низкий уровень внедрения и соблюдения политики кибербезопасности на уровне школ;

- недостаточная подготовка педагогов, администрации и учащихся в области цифровой безопасности.

Для снижения рисков и обеспечения соответствия требованиям кибербезопасности школьной системы проанализированные исследования описывают ряд ключевых механизмов комплаенс-менеджмента. В их числе:

- разработка и внедрение политики кибербезопасности на уровне образовательной организации, которая устанавливает обязательные правила, регламентирует порядок обработки данных и определяет ответственность участников процесса;

- стандартизация процедур киберзащиты, включая использование единых методик оценки угроз и внедрение современных технических решений для защиты данных;

- проведение самооценки и внешней оценки мер кибербезопасности, что позволяет школам выявлять слабые места и своевременно адаптировать стратегии защиты;

- обучение всех участников образовательного процесса — педагогов, администрации, технических специалистов, учащихся и родителей — основам кибергигиены, безопасного поведения в сети и реагирования на инциденты информационной безопасности.

Эти меры находят своё отражение в алгоритме комплаенс-менеджмента по кибербезопасности, который предполагает системный подход к управлению рисками: от анализа угроз и нормативных требований до внедрения политик, распределения ответственности и мониторинга эффективности мер защиты [92].

Анализ научной литературы также показал, что исследования в области комплаенс-менеджмента кибербезопасности в системе школьного образования пока крайне ограничены и носят фрагментарный характер. Это свидетельствует о недостаточной разработанности теоретической базы и подчёркивает актуальность проводимого исследования, направленного на создание научно обоснованных подходов и рекомендаций по организации киберзащиты школьных информационных систем.

## 2.2 Характеристика роли и места комплаенс-менеджмента в обеспечении кибербезопасности школьной образовательной среды

В последние годы вопросы кибербезопасности, развития IT-отрасли и повышения цифровой грамотности населения стоят особенно остро. С развитием информационно-коммуникационных технологий (ИКТ), причем темпами, опережающими формирование культуры их использования, растут и риски: как для граждан, так и для бизнеса и государственных органов. Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки, образования, социальные сети оказывают все более существенное влияние на развитие, поведение, ценностные ориентации и жизненные ориентиры современных детей и подростков, которые вполне самостоятельно формируют медиаконтент, определяют наиболее значимые медиасобытия в огромном информационном потоке.

Виртуальное взаимодействие, включающее онлайн-игры, переписку в чатах, участие в социальных интернет-сообществах, играет важную роль в жизни современных школьников. Основанием для активизации виртуальных контактов в социальных сетях становится близость интересов, общий круг общения, схожие представления о жизни и т.д. Вместе с тем, виртуальные контакты могут представлять опасности, связанные с различными видами виртуального преследования, демонстрацией сцен насилия и жестокости, возникновением зависимости и т.п. [93].

Чрезмерное увлечение интернет-сетями, как и в целом, использование интернет, может вызывать зависимость. Как и другие виды зависимости, интернет-аддикция оказывает разрушающее воздействие на школьника, негативно влияет на изменение физиологической, эмоциональной, поведенческой и личностной сферы [94]. Например, интернет-зависимый пользователь (в том числе и юный), как правило, находится в виртуальном пространстве дольше, чем он планировал, и продолжает ежедневно проводить там свое свободное время, несмотря на разрушительные последствия. У него постоянно возникает желание вернуться в сеть и посмотреть, какие изменения там произошли. Замещение реальных событий, которые происходят с ребенком в жизни на виртуальные иллюзии, отрицательно влияет и на состояние здоровья, и на успехи в учебе, и на характер реального общения. В связи с этим, родителям необходимо обращать пристальное внимание на дозирование времени, проведенного ребенком в Интернете.

Медианасилие оказывает негативное влияние на современную аудиторию – взрослых и особенно детей [95]. Это и изменения в поведении, связанные с агрессией и жестокостью; и смещение жизненных ценностей, где главным становится стремление

доминировать над окружающими людьми; и стремление подражать отрицательным героям в общении, манерах; и повышение риска криминогенного и асоциального поведения, и многие другие. Неслучайно защита детей от разрушительного влияния медианасилия понимается как важная социальная и государственная проблема *(отсылка на Киберщит)* [96].

Как обеспечить информационную безопасность в таких условиях, противостоять растущим киберугрозам, защитить персональные данные граждан, информационной инфраструктуры, стратегически важных объектов и, в целом, повысить защищенность национального информационного пространства? С целью решения всех этих поставленных задач в июне 2017 года Правительством была утверждена Концепция кибербезопасности «Киберщит Казахстана». Концепция основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития «цифровой» экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг. Документ определил основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий [96].

2 июля 2018 года был принят «О защите детей от информации, причиняющей вред их здоровью и развитию». Принятие данного закона направлено на «регулирование общественных отношений, возникающих в связи с реализацией прав детей на получение и распространение информации, направленных на защиту детей от информации, причиняющей вред их здоровью и развитию» [97].

Основными задачами настоящего Закона являются:

1) обеспечение защиты прав и законных интересов детей от информации, причиняющей вред их здоровью и развитию;

2) международное сотрудничество в сфере защиты детей от информации, причиняющей вред их здоровью и развитию.

Один из самых важных моментов, который регламентирует данный Закон – это прописанные компетенции государственных органов и местных исполнительных органов в сфере защиты детей от информации, причиняющей вред их здоровью и развитию и общественный контроль и участие в сфере защиты детей от информации, причиняющей вред их здоровью и развитию. Согласно данному пункту, Физические лица и некоммерческие организации вправе «осуществлять мониторинг распространения информационной продукции и доступа детей к информации, в том числе посредством создания и поддержания "горячих линий", применения технических, аппаратных и иных форм мониторинга и выявления информации,

информационной продукции и действий лиц, причиняющих вред здоровью и развитию детей» [97].

Таким образом, в условиях, когда защита детей от вредной информации возведена в ранг государственной задачи, становится очевидной необходимость системного подхода к обеспечению цифровой безопасности в образовательной среде. Одна из наиболее эффективных форм такой системной работы — внедрение комплаенс-менеджмента в сфере кибербезопасности. Он позволяет не только соответствовать требованиям законодательства, но и обеспечить постоянный внутренний контроль за цифровой средой школы, формируя культуру безопасного поведения в интернете у всех участников образовательного процесса.

В этой связи внедрение комплаенс-менеджмента в сфере кибербезопасности становится неотъемлемым элементом внутренней системы обеспечения информационной и психологической безопасности учащихся [98]. В рамках данной системы особое внимание уделяется разработке нормативных и методических документов, которые регламентируют поведение и ответственность всех участников образовательного процесса.

К ключевым элементам комплаенс-менеджмента относятся:

- стандарт по кибербезопасности, определяющий требования к технической защите информационной инфраструктуры школы;
- политика кибербезопасности, содержащая единые правила обращения с цифровыми ресурсами и данными;
- инструкции по кибербезопасности, описывающие конкретные действия сотрудников и учащихся при работе в цифровой среде и в случае киберинцидентов;
- система обучения и просвещения всех участников школьной жизни - педагогов, учеников и родителей — по вопросам цифровой гигиены, распознавания угроз и реагирования на потенциально опасные ситуации.

Таким образом, комплаенс-менеджмент формирует не просто формальный контроль, а культуру цифровой безопасности, основанную на знаниях, ответственности и взаимодействии всех участников школьного сообщества.

Информационная безопасность — одна из сфер комплаенса. Она включает создание и внедрение строгих процедур и технологий для защиты персональных данных, конфиденциальной информации и даже государственной тайны. Так как с развитием технологий возрастает количество угроз, таких как утечки данных, хакерские атаки и другие, внедрение комплаенс – менеджмента направлено на то, что образовательное учреждение принимает меры для предотвращения таких инцидентов и соблюдения законов в сфере защиты информации.

В настоящее время в мире существует большое количество подходов к обеспечению и управлению информационной безопасностью. Наиболее эффективные из них формализованы в виде международных стандартов и методологий, таких как ISO/IEC 27001, NIST Cybersecurity Framework, COBIT и другие [99]. Эти стандарты представляют собой универсальные инструменты, которые помогают организациям выстраивать системную работу по защите информации, определять риски, управлять ими и реагировать на инциденты.

Основные принципы, заложенные в международных стандартах, включают: принцип системного управления безопасностью, непрерывного совершенствования, ориентации на оценку рисков, разделения полномочий и ответственности, а также обеспечения конфиденциальности, целостности и доступности информации.

Благодаря своей универсальности, данные стандарты применимы в различных сферах, включая образование, где цифровая трансформация требует надежной защиты персональных данных, учебных материалов и цифровой инфраструктуры. Они служат ориентиром не только для крупных организаций, но и для образовательных учреждений, помогая выстроить эффективную и прозрачную политику в области кибербезопасности.

При этом для образовательных организаций, особенно на уровне средней школы, важно адаптировать эти международные подходы и стандарты к своему контексту, учитывая возрастные особенности учащихся, технические возможности и кадровые ресурсы. Реализация требований информационной безопасности в школьной среде требует создания понятной, структурированной и доступной системы внутренней документации, регламентирующей все аспекты цифрового взаимодействия.

Именно поэтому разработка нормативной базы и документации для обеспечения комплаенс-менеджмента в сфере кибербезопасности на уровне школы становится ключевым шагом в построении эффективной и устойчивой системы защиты информации и цифровой среды.

С учетом вышеописанных международных и национальных стандартов становится очевидным, что успешное обеспечение кибербезопасности в образовательной среде требует не просто формального соблюдения нормативных требований, но и создания четкой внутренней инфраструктуры цифровой безопасности.

Авторами был разработан системный пакет документов, предназначенных для внедрения комплаенс-менеджмента в школьную среду. Пакет включает в себя Стандарт обеспечения кибербезопасности образовательной среды школы, Положение о кибербезопасности, а также Политику кибербезопасности, которые адаптированы под реалии средней школы. Каждый из этих документов служит практическим инструментом для выстраивания

устойчивой и безопасной цифровой инфраструктуры, вовлекая в процесс не только педагогов и администрацию, но и родителей, учеников, технический персонал.

Стандарт по кибербезопасности представляет собой базовый нормативный документ, регламентирующий цели, задачи, принципы, терминологию и механизмы управления цифровой безопасностью в школьной системе. Он адаптирует положения международного стандарта ISO/IEC 27001 к условиям казахстанской школы и охватывает широкий спектр аспектов – от защиты информации и анализа рисков до формирования компетенций сотрудников и культуры киберответственности среди учащихся [100].

Положение о кибербезопасности школы детализирует стратегические и организационные механизмы управления цифровой безопасностью: распределение ответственности, принципы доступа, мониторинга, оценки рисков, а также ключевые задачи по реагированию на инциденты. Этот документ служит операционным руководством для повседневной работы всех участников школьного сообщества [101].

Политика кибербезопасности дополняет Положение и фокусируется на практических процедурах защиты информации, персональных данных, контроле доступа, использовании ИТ-оборудования и сетей. Она устанавливает конкретные правила поведения с цифровыми ресурсами, обеспечивая прозрачность и подотчетность всех действий в информационном пространстве школы.

Разработка и внедрение нормативной базы стало важным фундаментом для системного подхода к кибербезопасности в школьной среде. Однако одной только регламентации недостаточно для формирования по-настоящему устойчивой и безопасной цифровой культуры. Без осознанного участия и активного вовлечения всех участников образовательного процесса - учащихся, педагогов и родителей — любые меры останутся формальными. Именно поэтому следующим приоритетным направлением проекта стало создание обучающих материалов и просветительских инициатив, направленных на развитие цифровой грамотности и компетентности как основы современной кибербезопасности [103].

Для обеспечения системного и поэтапного внедрения мер по кибербезопасности в школах нами была разработана модель, которая отражает логику и последовательность ключевых шагов. Данная модель основана на принципах комплексного подхода и предполагает прохождение нескольких взаимосвязанных стадий: от подготовительного анализа до формирования устойчивой цифровой культуры. Визуально процесс можно представить в виде линейной последовательности, что позволяет наглядно продемонстрировать

движение от базовых организационных шагов к перспективным направлениям развития.

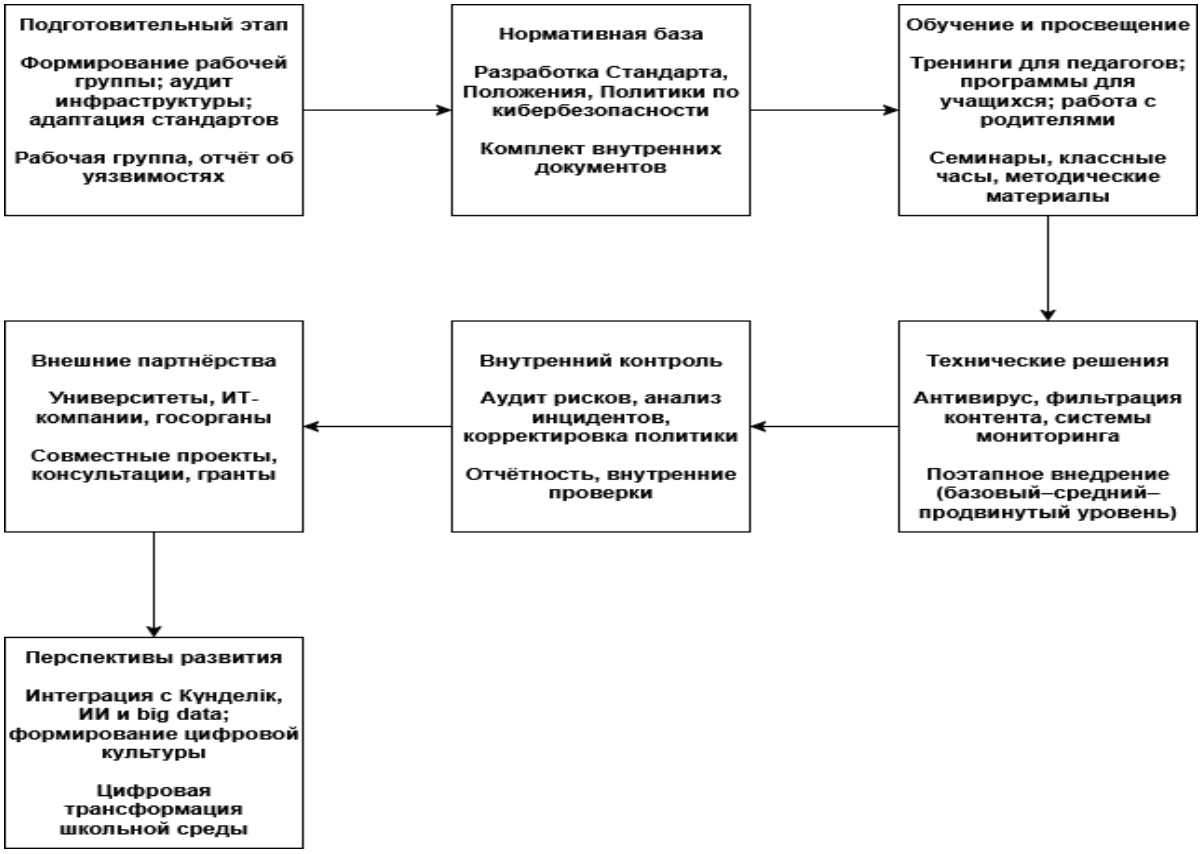



Рисунок 2.2.1 - Последовательность этапов построения системы кибербезопасности в школах

Представленный линейный процесс подчёркивает, что каждая стадия имеет не только самостоятельное значение, но и служит основой для последующих шагов. Таким образом, переход от нормативной базы к обучению, а затем к техническим решениям и внутреннему контролю обеспечивает целостность подхода. Особое внимание уделяется внешним партнёрствам и перспективам развития, что выводит стратегию за рамки формального соблюдения требований и формирует устойчивую цифровую экосистему в образовательной среде.

Владение фундаментальными принципами цифровой безопасности, способность анализировать критически источники информации онлайн, а также умение формировать и манипулировать цифровыми ресурсами – это ключевые компоненты цифровой компетентности. Цифровая компетентность не только обеспечивает возможность получения информации, но и способность аналитически мыслить, адекватно реагировать на онлайн-опасности, создавать материалы. Навык результативно применять технику обязателен для обучения, занятости и индивидуального роста. Для стимуляции

цифровой компетентности школьников необходимо применять различные приемы. Необходимо также стимулировать учащихся индивидуально изучать современные технологии и непрерывно улучшать свои умения. Школа играет важную функцию в развитии цифровых компетенций у обучающихся. Это обусловлено тем, что именно здесь дети впервые сталкиваются с серьезным применением (не у всех родители - программисты) компьютеров, сети Интернет и различных цифровых технологий. Преподаватели несут обязанность за то, чтобы образование охватывало не только стандартные предметы, но и занятия цифровой компетенцией.

Им необходимо преподавать учащимся основы цифровой гигиены в Интернете, основам кодирования, навыкам критического мышления при обработке данных в сети и прочим ключевым элементам цифровой грамотности. Требуется разрабатывать специализированные программы и учебные материалы, которые помогут учащимся освоить цифровые умения и стать компетентными в применении технологий [10]. Умение работать с оцифрованной информацией становится все более значимым навыком в настоящем обществе, особенно среди обучающихся. Впрочем, имеется целый ряд проблем и возможностей на пути их прогресса. Одно из основных испытаний - стремительное прогрессирование технических средств, что может привести к устареванию цифровых умений обучающихся. В связи с этим требуется регулярно обновлять учебные материалы и быть в курсе последних тенденций.

Иной проблемой может быть недостаточное побуждение самих учеников к развитию цифровой грамотности, поэтому крайне важно формировать увлекательные и прикладные задачи, которые будут поощрять их обучение. Впрочем, также имеются шансы – с расцветом веб-образования и опциями удаленного обучения обучающиеся способны получать возможность к различным образовательным источникам для улучшения цифровой грамотности. Основное - отыскивать равновесие между вызовами и перспективами, с тем чтобы эффективно продвигать у обучающихся значимые цифровые умения.

Внедрение комплаенс-менеджмента в школьную среду, несмотря на его стратегическую важность, сопровождается рядом вызовов и рисков, которые необходимо учитывать для достижения устойчивых результатов [98]. Одним из первых препятствий становится сопротивление со стороны учащихся и педагогов. Часто новые регламенты и контроль воспринимаются как ограничение свободы или дополнительная нагрузка, особенно если отсутствует предварительное разъяснение и вовлеченность в процесс. Ученики могут ощущать, что за ними ведётся чрезмерное наблюдение, что нарушает их личное пространство, особенно при введении ограничений на доступ к определённым интернет-ресурсам или

установке систем фильтрации контента. Педагоги, в свою очередь, могут воспринимать нововведения как вмешательство в их профессиональную автономию или как дополнительную ответственность, не связанную напрямую с их основной образовательной деятельностью. Недостаток цифровой грамотности у части педагогического состава также может вызывать опасения и внутреннее сопротивление к новым технологиям и требованиям. Кроме того, если внедрение проходит без чёткого объяснения целей и пользы, это способствует формированию негативного отношения и снижению мотивации к участию в программе. Для преодоления данного барьера важно выстраивать диалог, проводить обучающие сессии, акцентируя внимание не на контроле, а на защите, развитии и общем благе участников образовательного процесса.

Еще одной значимой проблемой являются технические и финансовые ограничения: не все школы обладают необходимыми ресурсами для приобретения лицензионного программного обеспечения, современных средств защиты или найма квалифицированных специалистов по ИТ-безопасности. Особенно остро эта проблема стоит в сельских и малокомплектных школах, где финансирование ограничено и отсутствует постоянный технический персонал. Даже при наличии базовой компьютерной инфраструктуры часто используются устаревшие устройства и неподдерживаемое программное обеспечение, что значительно повышает уязвимость киберсреды. Также школы нередко сталкиваются с отсутствием устойчивого интернет-соединения, что затрудняет реализацию программ дистанционного обучения и онлайн-контроля. Недостаточное финансирование мешает организовать регулярные обучающие мероприятия для педагогов и учеников по вопросам кибербезопасности. В результате возникает разрыв между потребностью в защите и фактическими возможностями по её обеспечению, что требует привлечения внешней поддержки, грантов, программ государственно-частного партнёрства и адаптации решений под доступные ресурсы. Дополнительную сложность представляет постоянно меняющийся характер киберугроз — технологии развиваются стремительно, а злоумышленники используют всё более изощрённые методы, что требует регулярного обновления политик, программ обучения и технических решений. Без постоянного мониторинга и гибкой адаптации к новым вызовам система комплаенс-менеджмента рискует устареть и потерять свою эффективность. Новые угрозы, такие как фишинг с элементами социальной инженерии, вредоносное ПО, замаскированное под легальные образовательные приложения, и атаки на системы видеосвязи, требуют нестандартных подходов к защите. Кроме того, школьники и студенты часто осваивают технологии быстрее педагогов, что создаёт дополнительную зону риска при отсутствии

своевременного реагирования со стороны администрации. Угрозы могут приходить не только извне, но и изнутри – в виде неосознанных действий самих пользователей, что делает особенно важным компонентом систему регулярного повышения осведомлённости. Сложность также заключается в необходимости согласовывать новые меры с существующими нормативными актами и инфраструктурными возможностями школы. Поэтому построение устойчивой и актуальной системы кибербезопасности требует постоянной аналитики, сотрудничества с экспертами и гибкости в управленческих решениях.

Внедрение комплаенс-менеджмента в сфере кибербезопасности школьной среды — это не разовая инициатива, а стратегически важное направление, требующее постоянного развития, адаптации и вовлеченности всех участников образовательного процесса. На основании проведенного анализа можно выделить ряд практических рекомендаций для школ [103].

Во-первых, необходимо начать с формирования рабочей группы, включающей представителей администрации, IT-специалистов и педагогов, которая займется разработкой и адаптацией нормативных документов. Создание рабочей группы — это первый и важнейший организационный шаг. В состав группы следует включить представителей администрации (директор, завучи), технических специалистов (системный администратор или IT-педагог), а также педагогов, активно использующих цифровые технологии. Такая междисциплинарная команда обеспечивает комплексный подход к кибербезопасности и позволяет учитывать как технические, так и педагогические аспекты. Группа отвечает за анализ текущей ситуации, выявление уязвимостей, адаптацию типовых документов (например, Положения и Политики по кибербезопасности), их внедрение и контроль исполнения.

Во-вторых, особое внимание следует уделить просветительской работе: регулярное проведение обучающих семинаров и тренингов по цифровой гигиене и кибербезопасности для учащихся, родителей и сотрудников. Один из главных факторов эффективности — информированность и мотивация участников. Необходимо регулярно проводить семинары, классные часы, родительские собрания и мастер-классы, направленные на формирование основ цифровой гигиены и киберответственности. Учащимся важно объяснять, как защитить личные данные, избегать фишинга и распознавать кибербуллинг. Родителей следует обучать безопасному поведению детей в сети и работе с родительским контролем [103]. Педагогов нужно готовить к использованию безопасных онлайн-ресурсов, цифровой этике и методам защиты информации в образовательной деятельности.

В-третьих, важно обеспечить поэтапное внедрение технических решений, начиная с базовых антивирусных программ и заканчивая

системами фильтрации и мониторинга активности в сети. Не каждая школа имеет возможность мгновенно внедрить весь спектр технических средств. Поэтому рекомендуется двигаться поэтапно.

На первом этапе — установка базового антивирусного ПО на все компьютеры, регулярное обновление систем и установка межсетевого экрана.

На втором этапе - настройка фильтров контента, систем родительского и сетевого контроля, создание резервных копий данных. На третьем этапе - внедрение более сложных решений: мониторинга сетевой активности, журналов безопасности, блокировок доступа к неавторизованным ресурсам и обучающих ИТ-платформ.

В-четвертых, следует наладить систему внутреннего контроля и отчетности, предусматривающую аудит рисков и анализ инцидентов с последующей корректировкой политики. Кибербезопасность — это процесс, а не единоразовое действие. Необходимо внедрить механизмы внутреннего контроля, включающие регулярные проверки соблюдения политик, анализ инцидентов, проведение внутренних аудитов безопасности и технических тестов на уязвимости. На основе собранных данных рабочая группа должна периодически пересматривать документацию, обновлять инструкции, изменять подходы и информировать коллектив о новых правилах. Это помогает оперативно реагировать на изменяющуюся ситуацию и сохранять актуальность мер защиты.

Наконец, необходимо поддерживать партнерства с университетами, экспертными организациями и государственными структурами, чтобы использовать доступные ресурсы и обновлять знания. Огромный ресурс для школ — это внешние партнёры. Сотрудничество с университетами, особенно педагогическими и техническими, даёт доступ к консультациям, обучающим материалам и волонтёрской поддержке. Экспертные организации и ИТ-компании могут предложить помощь в проведении оценки безопасности, предоставлении программного обеспечения или обучении персонала. Государственные структуры (например, министерство просвещения, управление образования) могут поддержать методическими рекомендациями и официальным сопровождением. Такое взаимодействие расширяет возможности школы и укрепляет её цифровую устойчивость.

Что касается перспектив дальнейшего развития, то система комплаенс-менеджмента будет развиваться в сторону интеграции с другими направлениями цифровой трансформации образования: электронным документооборотом, электронным дневником Кунделик, онлайн-обучения. Будущее также предполагает более широкое применение искусственного интеллекта и аналитики больших данных для мониторинга рисков в реальном времени. Не менее важно то, что с ростом цифровой культуры будет формироваться новое поколение

учащихся и педагогов, способных осознанно использовать технологии и защищать себя в цифровом пространстве. Таким образом, комплаенс-менеджмент становится не только инструментом контроля, но и основой для формирования безопасной, открытой и современной образовательной среды, отвечающей вызовам XXI века.

### 2.3 Анализ комплаенс-рисков в сфере кибербезопасности школьной образовательной среды

Процесс оценки всех видов рисков в сфере кибербезопасности является неотъемлемой частью процесса управления организацией в целом, поскольку определение и своевременная обработка неприемлемых рисков позволяет снизить вероятность нанесения как репутационного, так и материального ущерба. По сути, оценка рисков кибербезопасности сводится к определению как внешних, так и внутренних угроз, оценке влияния этих угроз на активы учебного заведения и подготовке аргументированного, с точки зрения возможных затрат, плана мероприятий по недопущению этих угроз.

В настоящее время существует множество методик по оценке рисков кибербезопасности – качественные и количественные, с различными методами по анализу рисков и различными способами для обработки неприемлемых рисков. Однако, в конечном итоге все эти методики сводятся к одному – определить неприемлемые риски и вовремя их обработать. При проведении анализа комплаенс-рисков в сфере кибербезопасности школьной образовательной среды рабочая группы был использован международный стандарт ISO/IEC 27005:2018 «Information technology - Security techniques - Information security risk management». Стандарт отражает следующие основные парадигмы:

1. Оценка рисков ведется с учетом последствий рисков для бизнес - процессов и вероятности возникновения рисков. Осуществляются идентификация рисков, их анализ и сравнение (с учетом выбранного уровня риск-толерантности).
2. Вероятность и последствия рисков доводятся до заинтересованных сторон и принимаются ими.
3. Устанавливается приоритет обработки рисков и конкретных действий по снижению рисков.
4. В процесс принятия решений по управлению рисками вовлекаются стейкхолдеры, которые затем также информируются о статусе управления рисками.
5. Оценивается эффективность проведенной обработки рисков.
6. Контролируются и регулярно пересматриваются риски и сам процесс управления ими.
7. На основе получаемой новой информации процесс управления рисками непрерывно улучшается.

8. Проводится обучение сотрудников и руководителей относительно рисков и предпринимаемых действий для их снижения (при имеющихся возможностях) [99].

Процесс управления рисками по ISO/IEC 27005:2018 состоит из следующих шагов (процессов), которые соответствуют подходу PDCA (Plan - Do - Check - Act):

1. Выбирается подход к управлению рисками, который должен включать в себя критерии оценки рисков, критерии оценки негативного влияния, критерии принятия рисков, оценка и выделение необходимых ресурсов.

2. Оценка рисков.

2.1 Идентификация рисков (инвентаризация активов, идентификация угроз, идентификация имеющихся мер защиты, определение уязвимостей, выявление последствий реализации угроз нарушения конфиденциальности / целостности / доступности ИТ-активов).

2.2 Проводится анализ рисков с различной глубиной, в зависимости от критичности активов, количества известных уязвимостей, а также с учетом ранее произошедших инцидентов. Методология анализа рисков может быть как качественной, так и количественной: как правило, вначале применяют качественный анализ для выделения высокоприоритетных рисков, а затем уже для выявленных рисков применяют количественный анализ, который является более трудоемким и дает более точные результаты.

2.3 Сравнение полученных на предыдущем этапе уровней рисков с критериями сравнения рисков и критериями принятия рисков, полученными на этапе определения контекста.

3. Обработка рисков кибербезопасности (модификация риска, сохранение риска, избегание риска, передача риска);

4. Формируется и утверждается руководством список принимаемых рисков;

5. Внедрение разработанного плана обработки рисков.

Закупаются и настраиваются средства защиты и оборудование, заключаются договоры киберстрахования и реагирования на инциденты, ведется юридическая работа с контрагентами.

6. Непрерывный мониторинг и пересмотр рисков

Риски могут незаметно меняться со временем: изменяются активы и их ценность, появляются новые угрозы и уязвимости, изменяются вероятность реализации угроз и уровень их негативного влияния.

7. Поддержка и улучшение процесса управления рисками кибербезопасности- контекст, оценка и план обработки рисков должны оставаться релевантными текущей ситуации и обстоятельствам [104].

Основной целью проведения данного анализа являлось определение комплаенс – рисков в сфере кибербезопасности школьной среды. Как было указано выше, были затруднения в доступе на базу определенной средней школы, поэтому были изучены и проанализированы общедоступные документы, сайты, нормативно-правовые акты. Весь процесс изучения выполнялся в соответствии с конфиденциальностью, целостностью и доступностью обрабатываемой информации. Рабочая группа пыталась идентифицировать как организационные, так и технические уязвимости образовательных учреждений Павлодарской области.

При формировании итогового реестра комплаенс-рисков в сфере кибербезопасности школьной образовательной среды, были выявлены следующие основные группы рисков:

1. Случайные. Объединяют непредвиденные события, когда происходит стечение обстоятельств, приводящее к неблагоприятным последствиям. Как правило, это внезапные, сложно прогнозируемые риски разного характера. Среди типичных примеров – выход из строя технического оборудования, ЧС, перебои электроэнергии, повреждение коммуникационных каналов, поломка блокирующих устройств, ограничивающих доступ к информации.
2. Субъективные. Возникают из-за ошибок и неправильных действий персонала при обработке, хранении информации. Типичными ситуациями здесь выступают пренебрежение внутренними правилами и регламентом безопасности в компании: нарушение режима тайны, несанкционированный доступ к сведениям, нарушение правил передачи информации, использование незащищенных информационных каналов.
3. Объективные. Возникают в ходе использования защитных систем и сопутствующего технического оборудования. Риски возникают в результате проникновения в информационную систему вредоносного ПО, внедрения следящего, шпионского оборудования. Подобные риски отличаются невозможностью полного исключения ввиду несовершенства защиты, многообразия приемов злоумышленников.

В таблице 2.3.1 описаны риси кибербезопасности в школьной образовательной среде.

Талица 2.3.1 - Реестр рисков кибербезопасности

| № | Наименование риска | Уровень риска |
|---|---|---|
| 1 | Использование вредоносных программного обеспечения, нелегальных программ | Высокий |
| 2 | Хакерские атаки, фишинг | Высокий |
| 3 | Утечка персональных данных сотрудников | Высокий |
| 4 | Обход средств защиты с целью получить | Высокий |

| | | |
|---|---|---|
| | несанкционированный доступ к информационным системам и данным (исходит от сотрудников учреждения) | |
| 5 | Разглашение конфиденциальных сведений | Высокий |
| 6 | Кража внутренней (служебной) информации, хищение данных | Средний |
| 7 | Вывод из строя оборудования и систем | Высокий |
| 8 | Доступность публичных сервисов | Средний |
| 9 | Потеря (уничтожение) данных из-за возможности физической поломки в компьютере | Высокий |
| 10 | Заражение вредоносным программным обеспечением из-за возможности открытия зараженных, вредоносных файлов в операционной системе и наличия технических (программных) уязвимостей | Средний |
| 11 | Потеря доступа в Интернет по причине провайдера | Средний |
| 12 | Прекращение работы средства защиты информации, антивирусных программ из-за невозможности приобретения (закупки) | Средний |
| 13 | Раскрытие ключей (паролей) доступа | Низкий |
| 14 | Утечка информации из-за возможности доступа к некорпоративным облачным хранилищам в локальной сети | Высокий |
| 15 | Нарушение законодательства о коммерческой тайне из-за отсутствия соглашений (обязательств) о конфиденциальности у работника | Средний |
| 16 | Нехватка квалифицированных ИТ – специалистов по причине отсутствия ставок в структуре образовательного учреждения | Высокий |
| 17 | Перехват управления социальными сетями из-за возможности подбора пароля в представительстве в социальных сетях или из-за увольнения ответственного за социальные сети работника | Низкий |
| 18 | Неработоспособность серверного оборудования | Низкий |
| 19 | Обход систем защиты из-за отсутствия контроля за изменением конфигурации в средстве защиты информации | Средний |
| 20 | Физическое повреждение оборудования из-за недостаточного технического обслуживания в оборудовании или из-за износа компонентов в оборудовании | Высокий |
| 21 | Неработоспособность операционной системы | Средний |
| 22 | Неработоспособность локальной сети из-за отсутствия электропитания в сетевом оборудовании | Высокий |
| 23 | Повреждение коммуникаций вроде водоснабжения | Высокий |

| | | |
|---|---|---|
| | или электроснабжения, а также вентиляции, канализации | |
| 24 | Неисправность и устаревание отдельных элементов (размагничивание носителей данных, таких как дискеты, кабели, соединительные линии и микросхемы) | Средний |
| 25 | Неисправность в работе ограждающих устройств (заборы, перекрытия в здании, корпуса оборудования, где хранится информация) | Средний |

По результатам проведенного анализа комплаенс-рисков в сфере кибербезопасности школьной образовательной среды предпринимаются следующие способы нейтрализации угроз кибербезопасности:

- Внедрение принципа минимальных привилегий, то есть назначить сотрудникам только те полномочия, которых достаточно для выполнения обязанностей.
- Формирование у сотрудников культуры информационной безопасности, рассказать о возможных угрозах и способах защиты от них.
- Введение четких регламентов, касающиеся каналов передачи информации (например, запрет на использование съемных носителей).
- Передача данных в зашифрованном виде, чтобы злоумышленники не могли их прочитать и использовать в своих целях.
- Проведение внутренних анализов рисков кибербезопасности в каждом отдельно взятом образовательном учреждении на ежегодной основе.
- Своевременная реакция на инциденты кибербезопасности, можно предпринять соответствующие меры по недопущению этих инцидентов и тем самым предотвратить возможный ущерб.

Таким образом, анализ рисков кибербезопасности в школьной образовательной среде позволил определить реестр и уровень опасности, что, в свою очередь, определяет действия по выбору способам нейтрализации угроз кибербезопасности в школе.

## 2.4 Характеристика применяемых в школе защитных средств кибербезопасности

Школы используют различные средства кибербезопасности для защиты своей цифровой среды, которая становится все более уязвимой к киберугрозам из-за интеграции технологий в образование. Эти средства защиты включают как технологические меры, так и образовательные стратегии, направленные на снижение рисков и

повышение осведомленности учащихся и персонала о безопасности. В следующих разделах подробно описаны основные средства защиты от кибербезопасности, используемые в школах, на основе предоставленных исследовательских работ.

С технологической точки зрения, образовательные учреждения всё чаще внедряют облачные технологии и используют сегрегированные сети, такие как виртуальные локальные сети (VLAN), что позволяет изолировать конфиденциальные данные и снизить риск несанкционированного доступа к ресурсам школы. Одновременно всё более распространённой практикой становится применение двухфакторной аутентификации, которая усиливает защиту пользовательских учётных записей, поскольку требует дополнительной верификации при входе в систему, помимо ввода пароля [105]. Существенное развитие получили системы безопасности на основе искусственного интеллекта, которые позволяют в режиме реального времени обнаруживать потенциальные угрозы и аномальное поведение в сети, тем самым значительно снижая вероятность успешных кибератак на школьные ресурсы [106].

К базовым средствам защиты относятся также брандмауэры и антивирусное программное обеспечение, которые обеспечивают фильтрацию сетевого трафика, предотвращение несанкционированного доступа и блокировку вредоносного программного обеспечения, защищая школьные информационные системы от внешних угроз [107]. Особое внимание уделяется шифрованию данных и строгому контролю доступа к цифровым образовательным платформам и хранилищам, что позволяет обеспечить конфиденциальность и целостность информации, включая персональные данные учащихся, педагогов и сотрудников администрации [108].

В результате анализа обеспечения кибербезопасности школьной среды было определено, что для настройки доступа к сети интернет в школах (организациях образования, где обучаются учащиеся до 18 лет) как правило применяются специальные DNS сервера, в которых прописаны только доступные ресурсы, а также постоянно пополняющийся список заблокированных сайтов, содержащих в себе ненормативную информацию.

Кроме того, для обеспечения безопасности при передаче логинов и паролей по сети необходимо использовать сервисы шифрования (протоколы шифрования) - SSL-сертификаты. Поэтому при создании и разработке в организации образования своего портала, в котором обязательно должна присутствовать авторизация логином и паролем обязательно данный домен должен содержать SSL-сертификат. АО «Казахтелеком» для предоставления безопасного интернета в организации образования предоставляет «зеленый интернет». В крупных организациях используется корпоративное шифрование

через радиосервер. Настройка DNS осуществляется после закупа как провайдером, когда он настраивает свой шлюз, так и учреждениям образования. В школе эту работу выполняет системный администратор. Он указывает свой внешний IP-адрес, который может быть как динамичным, так и статичным, а также указывает DNS-серверы. Как правило DNS-серверы «зеленого интернета». При настройке WI-FI сети указываются следующие параметры: 1) радиосервер, когда нужна обязательная авторизация пользователя 2) настройка пароля от админ-панели (используется WEB-шифрование 16-битным кодом) 3) скрытые SSID (когда закрытая WI-FI сеть не видна). Использование WI-FI сетей без пароля запрещены.

Во многих исследованиях отмечается, что технологические меры без сопровождения обучения и понятных инструкций остаются недостаточно использованными. Пользователи могут технически иметь возможность шифрования, но часто игнорируют или неправильно настраивают такие функции. Сетевые механизмы вроде VLAN и сегрегации сети являются мощным средством защиты, однако их внедрение зависит от наличия компетентного персонала и ресурсов для поддержки инфраструктуры. Использование стандартов TLS/SSL, PGP/S/MIME и E2EE является признанным мировым лучшим практическим подходом, но их эффективность в школьной среде требует адаптации к условиям: нужно обеспечить удобство, управляемость ключами, совместимость с используемыми платформами и понимание среди пользователей.

В образовательной среде, в том числе в школах, использование криптографических протоколов и защитных средств имеет важное значение для защиты конфиденциальных данных учеников, учителей и администрации. Это особенно важно при обработке и передаче персональных данных, учебной документации и другой чувствительной информации. Основными средствами защиты информации в школах являются различные криптографические протоколы и методы шифрования, которые обеспечивают целостность и конфиденциальность данных.

Наряду с техническими средствами значительная роль в обеспечении киберзащиты школ принадлежит образовательным стратегиям и программам повышения цифровой грамотности. Многие учреждения реализуют целевые программы по обучению учащихся и сотрудников основам кибербезопасности, включая методы распознавания фишинговых атак, создание надёжных паролей и безопасное использование цифровых платформ [108]. Всё чаще внедряются курсы по киберэтике и ответственному поведению в цифровой среде, способствующие формированию культуры безопасного использования технологий [109]. Кроме того, особое внимание уделяется непрерывному повышению квалификации педагогов и административного персонала, чтобы обеспечить

готовность работников образовательных организаций к предотвращению и устранению киберинцидентов, а также к управлению возможными угрозами [104].

Важной составляющей эффективной киберзащиты является соблюдение нормативных требований и разработка политики информационной безопасности. Все больше школ внедряют системы управления соответствием стандартам киберзащиты, что способствует унификации процессов защиты данных и приведению практик к требованиям национальных и международных регламентов. В рамках таких инициатив разрабатываются и применяются комплексные политики кибербезопасности, определяющие правила использования цифровых технологий, порядок обработки персональных данных и меры предотвращения утечек конфиденциальной информации [110].

Несмотря на широкое использование современных средств киберзащиты, образовательные учреждения сталкиваются с рядом существенных проблем, ограничивающих их эффективность. Среди основных вызовов выделяются ограниченность бюджетных ресурсов, нехватка квалифицированных специалистов и недостаточная поддержка со стороны руководства школ при внедрении сложных технических решений [111]. Кроме того, серьёзной угрозой остаётся человеческий фактор: многочисленные исследования подтверждают, что значительная часть киберинцидентов в школах происходит из-за ошибок пользователей, недостатка знаний и [112].

Таким образом, обеспечение кибербезопасности в школьной среде требует комплексного подхода, который сочетает современные технологические решения, образовательные стратегии и эффективные механизмы комплаенс-менеджмента. Только интеграция технических, организационных и педагогических мер позволит создать устойчивую, безопасную и надёжную цифровую образовательную экосистему, способную противостоять растущему количеству угроз в информационном пространстве.

# ГЛАВА 3. ПЕДАГОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗО-ПАСНОСТИ В ШКОЛЬНОЙ СРЕДЕ

## 3.1 Нормативные документы для организации кибербезопасности в школьной среде

Кибербуллинг, фишинг и другие виды киберугроз, которые существуют в современном цифровом мире могут потенциально затронуть большинство детей и взрослых. Соответственно, сохранение безопасности в школе и в повседневной жизни важна для обеспечения безопасности людей. Целью данного пункта является определение ключевых показателей минимальных стандартов для программ готовности к сохранению кибербезопасности в школьной среде. Зададимся вопросом «Какие существуют в Казахстане нормативные документы, регламентирующие сохранение кибербезопасности в школьной среде?».

Для достижения цели была изучена база нормативных документов на сайте adilet.kz. В качестве нормативных документов были проанализированы законы Республики Казахстан, стандарты, положения и приказы. В данном разделе приведены нормативные ссылки на акты законодательства, а также их описание.

Цели и принципы стандартизации в сфере кибербезопасности в Республике Казахстан установлены в Национальном стандарте РК «СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования» и в «Единых требованиях в области информационно-коммуникационных технологий и обеспечения информационной безопасности», утвержденными Постановлением Правительства Республики Казахстан от 20 декабря 2016 года [113].

*I Законодательство*

1. Закон Республики Казахстан от 24.11.2015 г. «Об информатизации» [114].

Данный закон регулирует общественные отношения в сфере информатизации, возникающие на территории Республики Казахстан между государственными органами, физическими и юридическими лицами при создании, развитии и эксплуатации объектов информатизации, а также при государственной поддержке развития отрасли информационно-коммуникационных технологий.

Основные понятия: Закон вводит определения таких терминов, как «информатизация», «информационно-коммуникационные технологии (ИКТ)», «информационная безопасность», «объекты информатизации» и другие, что создает единое понятийное поле для регулирования сферы ИКТ.

Цели и принципы: Устанавливаются цели государственного регулирования в сфере информатизации, включая формирование и развитие информационного общества, обеспечение информационной безопасности личности, общества и государства, а также развитие отечественной отрасли ИКТ.

Государственное управление: Определяются компетенции Правительства Республики Казахстан, уполномоченных органов и местных исполнительных органов в сфере информатизации, включая разработку и реализацию государственной политики, координацию деятельности в области ИКТ и обеспечение информационной безопасности.

Информационная безопасность: Закон подчеркивает необходимость обеспечения безопасности информационных систем, включая защиту персональных данных и предотвращение несанкционированного доступа к информации.

Развитие цифровой грамотности: Одной из задач государственного управления в сфере информатизации является повышение цифровой грамотности населения, что включает в себя обучение основам безопасного использования ИКТ.

Закон «Об информатизации» служит нормативной основой для внедрения и развития проактивного обучения кибербезопасности в средней школе [115]. В частности:

– Правовая база: Закон предоставляет юридические основания для разработки и реализации образовательных программ по кибербезопасности, направленных на формирование у учащихся навыков безопасного поведения в цифровой среде.

– Государственная поддержка: Установленные в законе задачи по повышению цифровой грамотности населения и обеспечению информационной безопасности отражают приоритетность данных направлений в государственной политике, что способствует поддержке инициатив в области проактивного обучения кибербезопасности.

– Интеграция ИКТ в образование: Закон стимулирует внедрение ИКТ в образовательный процесс, что создает условия для использования цифровых инструментов и ресурсов в обучении кибербезопасности.

– Защита информации: Подчеркивая важность информационной безопасности, закон акцентирует внимание на необходимости формирования у учащихся понимания угроз в цифровой среде и способов их предотвращения.

Закон Республики Казахстан «Об информатизации» является ключевым нормативным документом, определяющим направления развития информационного общества и обеспечения информационной безопасности. Его положения создают благоприятные условия для внедрения проактивного обучения кибербезопасности в средней

школе, обеспечивая правовую и организационную поддержку соответствующих образовательных инициатив.

2. Закон Республики Казахстан от 05.07.2004 г. «О связи» [116].

Закон Республики Казахстан от 5 июля 2004 года № 567-II «О связи» устанавливает правовые основы деятельности в области связи на территории Республики Казахстан. Он определяет полномочия государственных органов по регулированию данной деятельности, а также права и обязанности физических и юридических лиц, оказывающих или пользующихся услугами связи.

Основные положения закона:

– Назначение связи: Связь признается неотъемлемой частью экономической и социальной инфраструктуры страны, предназначенной для удовлетворения потребностей физических и юридических лиц, а также обеспечения безопасности, обороны и охраны правопорядка.

– Государственное регулирование и контроль: Государственное управление в области связи осуществляется Президентом, Правительством и уполномоченным органом. Контроль за соблюдением законодательства в области связи возлагается на уполномоченный орган и его территориальные подразделения.

Основные принципы регулирования: Включают защиту прав пользователей, обеспечение равенства прав на участие в деятельности в области связи, содействие добросовестной конкуренции, обеспечение безопасности и надежности связи, а также интеграцию в мировую систему связи.

Компетенция государственных органов:

– Правительство: Разрабатывает основные направления государственной политики в области связи, утверждает порядок подготовки и использования сетей телекоммуникаций общего пользования.

– Уполномоченный орган: Осуществляет лицензирование деятельности в области связи, контроль за качеством услуг, утверждение правил регистрации абонентских устройств и другие функции.

– Лицензирование и использование ресурсов: Закон устанавливает порядок лицензирования деятельности в области связи и распределения национальных ресурсов, таких как радиочастотный спектр и нумерация.

– Права пользователей: Гарантируется право на получение качественных услуг связи, защита персональных данных и тайны связи, а также возможность выбора оператора связи.

– Ответственность: Закон предусматривает ответственность операторов и пользователей за нарушение законодательства в области

связи, включая возможность приостановления работы сетей и (или) средств связи в случае нарушений.

Этот закон является ключевым нормативным актом, регулирующим сферу связи в Республике Казахстан, и обеспечивает правовую основу для развития и функционирования телекоммуникационной инфраструктуры страны.

*II Постановления Правительства Республики Казахстан*

Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 утвердило Концепцию цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы [117]. Этот стратегический документ определяет направления цифрового развития Казахстана, включая усиление кибербезопасности и внедрение инновационных технологий в различные сферы жизни.

Основные положения Концепции:

Цели и задачи:

– Обеспечение устойчивого цифрового развития страны.
– Развитие информационно-коммуникационных технологий (ИКТ).
– Укрепление кибербезопасности.
– Повышение цифровой грамотности населения.

Ключевые направления:

– Цифровая трансформация: внедрение цифровых технологий в государственное управление, экономику и социальную сферу.
– Развитие ИКТ: создание благоприятных условий для развития ИКТ-сектора, включая поддержку стартапов и инновационных проектов.
– Кибербезопасность: разработка и реализация мер по защите информационных систем и данных от киберугроз.

Целевые индикаторы:

– Достижение определённых позиций в международных рейтингах по уровню цифровизации и кибербезопасности.
– Увеличение доли населения, обладающего цифровыми навыками.
– Рост объёма цифровых услуг, предоставляемых государством.

Механизмы реализации:

– Разработка и внедрение нормативных правовых актов, регулирующих цифровую сферу.
– Создание инфраструктуры для поддержки цифровых инициатив.
– Обеспечение межведомственного взаимодействия и координации действий в сфере цифровизации.

– Концепция служит основой для формирования государственной политики в области цифровой трансформации и кибербезопасности, направленной на повышение конкурентоспособности Казахстана в глобальном цифровом пространстве.

4. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 утвердило Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности [118]. Этот нормативный акт разработан в соответствии с подпунктом 3) статьи 6 Закона Республики Казахстан «Об информатизации» и направлен на установление обязательных требований в сфере ИКТ и информационной безопасности для государственных органов, субъектов квазигосударственного сектора и владельцев критически важных объектов информационно-коммуникационной инфраструктуры.

Основные положения документа:

Цель и задачи:

– Установление единых требований в области ИКТ и информационной безопасности.

– Определение принципов организации и управления информатизацией государственных органов.

– Повышение уровня защищенности электронных информационных ресурсов и информационных систем.

– Сервис управления безопасностью SECURITM

Область применения:

Требования обязательны для государственных органов и местных исполнительных органов, государственных юридических лиц, субъектов квазигосударственного сектора, собственников и владельцев негосударственных информационных систем, интегрируемых с государственными системами или предназначенных для формирования государственных электронных информационных ресурсов, собственников и владельцев критически важных объектов информационно-коммуникационной инфраструктуры.

Основные требования:

– Унификация компонентов информационно-коммуникационной инфраструктуры.

– Стандартизация структуризации ИКТ-инфраструктуры и организация серверных помещений.

– Обязательное применение рекомендаций стандартов в области ИКТ и информационной безопасности на всех этапах жизненного цикла объектов информатизации.

– Разработка и внедрение технической документации по информационной безопасности, включая политику ИБ, методики

оценки рисков, правила идентификации и классификации активов, процедуры внутреннего аудита и другие.

Мониторинг и контроль:

– Организация системы мониторинга обеспечения информационной безопасности.

– Ведение журналов регистрации событий информационной безопасности.

– Разработка планов мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации.

Постановление № 832 служит основой для формирования и реализации политики в области информатизации и информационной безопасности, обеспечивая единый подход к управлению ИКТ и защите информации в Республике Казахстан.

5. Постановление Правительства Республики Казахстан от 9 августа 2018 года № 488 утвердило Национальный антикризисный план реагирования на инциденты информационной безопасности [119]. Этот документ определяет порядок действий субъектов системы по снижению влияния инцидентов информационной безопасности и минимизации нарушений их работы.

Основные положения документа:

1. Цель и задачи:

– Установление порядка действий субъектов системы по снижению влияния инцидентов информационной безопасности.

– Минимизация нарушений работы информационно-коммуникационной инфраструктуры.

2. Область применения:

– План распространяется на:

– Государственные органы и местные исполнительные органы.

– Государственные юридические лица.

– Субъектов квазигосударственного сектора.

– Собственников и владельцев критически важных объектов информационно-коммуникационной инфраструктуры.

3. Основные требования:

– Разработка и утверждение планов реагирования на инциденты информационной безопасности.

– Организация и проведение профилактических мероприятий.

– Мониторинг состояния информационной безопасности.

– Взаимодействие с Национальным координационным центром информационной безопасности (НКЦИБ).

4. Мониторинг и контроль:

– Организация системы мониторинга обеспечения информационной безопасности.

– Ведение журналов регистрации событий информационной безопасности.

– Разработка планов мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов.

Постановление № 488 служит основой для формирования и реализации политики в области реагирования на инциденты информационной безопасности, обеспечивая единый подход к управлению ИКТ и защите информации в Республике Казахстан.

Национальный антикризисный план реагирования на инциденты информационной безопасности является важной стратегической и нормативной основой для построения системы проактивного обучения кибербезопасности в средней школе.

Во-первых, документ раскрывает структурированный алгоритм реагирования на инциденты, который может быть адаптирован для педагогических целей — например, при разработке учебных ситуаций, тренингов и ролевых игр для школьников. Знание базовых принципов антикризисного реагирования позволяет обучать учащихся действовать по сценарию, не теряя времени и правильно реагируя на угрозы в интернете.

Во-вторых, постановление подчёркивает необходимость профилактики и планирования действий до возникновения инцидентов, что полностью соответствует проактивному подходу в обучении, ориентированному не на «реагирование постфактум», а на предупреждение и минимизацию рисков.

В-третьих, документ подчёркивает важность взаимодействия разных участников цифровой среды (госструктуры, организации, пользователи) при реагировании на угрозы. Это может быть положено в основу обучения школьников правилам совместной ответственности и цифровой гигиены, как части культуры коллективной безопасности в школе и семье.

Таким образом, Национальный антикризисный план не только задаёт стандарты для госорганов и организаций, но и может использоваться как образец для формирования у школьников практических навыков реагирования на киберугрозы через моделирование инцидентов, обучение сценарному поведению и развитие цифровых компетенций.

*III Приказы государственных органов Республики Казахстан*

В рамках реализации государственной политики в области цифровизации и информационной безопасности в Республике Казахстан приняты подзаконные акты, регламентирующие порядок функционирования, мониторинга, контроля, экспертизы и защиты информационных систем и инфраструктуры.

Среди таких актов выделяются приказы, направленные на обеспечение:

1. Осуществляется мониторинг инцидентов информационной безопасности и реализация механизмов реагирования. Для информационных систем государственных органов, объектов «электронного правительства», а также критически важных объектов информационно-коммуникационной инфраструктуры установлены регламентированные правила наблюдения за событиями и инцидентами в сфере информационной безопасности (приказы № 52/НҚ, № 199/НҚ). Регламентировано взаимодействие между оперативными центрами информационной безопасности и Национальным координационным центром (приказ № 48/НҚ).

2. Функционирования ключевой цифровой инфраструктуры. Определены правила функционирования единого шлюза доступа в Интернет и почтового шлюза «электронного правительства» (приказ № 386/НҚ). Установлены правила присоединения сетей операторов связи и пропуска интернет-трафика, что влияет на управление интернет-трафиком в стране (приказ № 24/нс). Введены требования к функционированию централизованного управления сетями телекоммуникаций (приказ № 25/нс). Регламентировано ведение реестра статических IP-адресов, что важно для управления цифровыми идентификаторами в сети (приказ № 400/НҚ).

3. Резервного копирования и хранения информации. Установлены правила создания и функционирования единой национальной платформы резервного хранения данных и передачи на неё копий электронных информационных ресурсов (приказы № 44/НҚ, № 45/НҚ). 4. Экспертизы и оценки защищенности объектов информатизации Определён порядок проведения испытаний и экспертиз информационных систем на соответствие требованиям ИБ, в том числе инвестиционных предложений в сфере информатизации (приказы № 111/НҚ, № 144/НҚ). Закреплены правила разработки и утверждения технических заданий на создание и развитие объектов информатизации (приказ № 143/НҚ).

5. Защиты персональных данных. Определён порядок обследования защищенности персональных данных в электронных ресурсах, что является критически важным для соблюдения конфиденциальности информации о пользователях (приказ № 156/НҚ). 6. Видеомониторинга и безопасности в общественных местах. Установлены правила функционирования Национальной системы видеомониторинга, как части общей системы обеспечения безопасности в цифровой и физической среде (приказ № 69-қе).

Совокупность указанных приказов создаёт регулятивную и методическую основу для:

– Формирования у учащихся знаний о принципах функционирования цифровой инфраструктуры, включая интернет-доступ, хранение данных, защиту информации и управление трафиком.

– Обучения навыкам проактивного поведения в цифровой среде, включая осознанное отношение к личным данным, безопасному использованию сетей и цифровых сервисов.

– Разработки учебных кейсов и тренингов, основанных на реальных нормативных требованиях к защите информации и реагированию на инциденты.

– Повышения цифровой грамотности и культуры безопасности школьников, через знакомство с государственными мерами и системами, обеспечивающими киберзащиту на уровне страны.

Таким образом, данные приказы позволяют встроить практико-ориентированные модули в содержание обучения кибербезопасности в школе, основываясь на реальных государственных стандартах и регламентированных процедурах.

*IV Стандарты*

В Республике Казахстан приняты национальные стандарты, устанавливающие требования к проектированию, управлению и обеспечению информационной безопасности информационных систем и сетей. Эти стандарты направлены на формирование единого подхода к защите информации и минимизации киберугроз.

1. Стандарты по управлению процессами разработки и стандартизации информационных систем:

– СТ РК 1.15-2019 регламентирует порядок создания и деятельности технических комитетов по стандартизации, что обеспечивает системный подход к разработке стандартов в ИКТ-сфере.

– СТ РК 34.015-2002 устанавливает требования к техническим заданиям на создание автоматизированных систем, что важно для планирования безопасных образовательных цифровых решений.

2. Стандарты по системам управления информационной безопасностью:

В числе ключевых международных и национальных стандартов, направленных на развитие культуры информационной безопасности, особое место занимают СТ РК ISO/IEC 27001-2023 и СТ РК ISO/IEC 27002-2015.

СТ РК ISO/IEC 27001-2023 устанавливает требования к созданию и функционированию системы менеджмента информационной безопасности (СМИБ). Стандарт описывает структурированный подход к управлению информационными рисками, включая процессы идентификации угроз, оценки уязвимостей, контроля доступа, мониторинга событий безопасности и реагирования на инциденты. Реализация требований данного стандарта позволяет организациям выстраивать управляемую, непрерывно совершенствующуюся систему обеспечения безопасности

информации, что делает его основой для построения комплексной политики информационной безопасности.

В развитие положений ISO/IEC 27001 действует СТ РК ISO/IEC 27002-2015, который представляет собой свод практических рекомендаций и мер по защите информации, включая как организационные, так и технические средства безопасности. В этом стандарте описаны методы управления персоналом, доступа к информации, физической и сетевой безопасностью, а также политики использования информационных систем. Данный свод правил помогает конкретизировать, как именно реализовать требования ISO/IEC 27001 на практике.

Дополняет указанные стандарты СТ РК ISO/IEC 13335-5-2008, который предлагает руководство по управлению защитой сетевой инфраструктуры, включая средства контроля доступа, защиты сетевых соединений, мониторинга трафика и реагирования на сетевые угрозы. Этот стандарт особенно важен в условиях сетевой интеграции образовательных учреждений, где школьные сети взаимодействуют с внешними информационными ресурсами, что требует повышения уровня сетевой безопасности.

Особое место в системе международных стандартов занимают СТ РК ISO/IEC 15408-1-2017, 15408-2-2017 и 15408-3-2017 (известные как Common Criteria). Эти документы определяют критерии оценки безопасности информационных технологий. Первая часть представляет общую модель и терминологию, вторая — функциональные требования, предъявляемые к ИТ-продуктам и системам, а третья — требования к процессам разработки, тестирования и сертификации. Данные стандарты широко применяются для независимой оценки безопасности информационных систем, подтверждая их соответствие международным требованиям.

Эти стандарты применяются для оценки и сертификации ИТ-продуктов и систем на соответствие заданным требованиям безопасности.

Перечисленные стандарты:

– Обеспечивают методическую основу для формирования представлений у школьников о требованиях к безопасности цифровых систем и сетей.

– Позволяют внедрять в образовательную практику мировые подходы к управлению информационной безопасностью и оценке рисков.

– Способствуют формированию у учащихся прикладных знаний о системных требованиях к кибербезопасности и необходимости стандартизации в цифровой сфере.

– Могут служить основой для разработки учебных материалов и тренингов, направленных на развитие у школьников практических навыков защиты информации.

Актуализируют важность планирования и проектирования безопасных цифровых образовательных решений, что соответствует проактивному подходу.

Таким образом, использование данных стандартов в содержании обучения способствует развитию у школьников системного и осознанного отношения к вопросам кибербезопасности, ориентируя их на профилактику цифровых угроз в соответствии с международными и национальными требованиями.

Проведённый анализ законодательства, подзаконных актов и стандартов Республики Казахстан в области цифровизации, информатизации и информационной безопасности показал, что в стране сформирована разветвлённая нормативно-правовая база, регулирующая ключевые аспекты:

– цифровой трансформации и развития информационно-коммуникационных технологий (ИКТ);

– обеспечения кибербезопасности на уровне государственных органов, квазигосударственного сектора и критически важных объектов инфраструктуры;

– управления информационными рисками и реагирования на инциденты информационной безопасности;

– внедрения международных стандартов в области менеджмента информационной безопасности и защиты сетевой инфраструктуры.

Принятые законы, постановления Правительства, приказы уполномоченных органов и национальные стандарты позволяют выстраивать системный подход к обеспечению информационной безопасности на уровне государственных и корпоративных структур. Эти документы закладывают основы государственной политики в сфере цифровизации и кибербезопасности, формируют требования к инфраструктуре, процессам мониторинга и реагирования, а также к управлению рисками и защите информации.

Для разработки теоретико-методологических основ проактивного обучения кибербезопасности в средней школе указанные документы являются важной основой, поскольку позволяют:

– интегрировать принципы государственной политики в образовательный процесс;

– разрабатывать учебные программы, основанные на реальных требованиях к безопасности информации;

– формировать у школьников практические навыки предупреждения и предотвращения цифровых угроз;

– обеспечить соответствие содержания обучения актуальным национальным и международным стандартам.

Выявленные ограничения и недостатки

Вместе с тем проведённый анализ показывает, что существующая нормативная база преимущественно ориентирована на государственные органы, квазигосударственный сектор, крупные предприятия и инфраструктурные объекты.

Система школьного образования как самостоятельная часть информационной инфраструктуры в этих документах практически не представлена.

Отсутствуют специальные нормативные акты и методические рекомендации, направленные на регулирование вопросов кибербезопасности именно в школьной среде, включая:

– разработку и внедрение школьных программ по кибербезопасности;

– обеспечение безопасности школьных информационных систем и сетей;

– организацию профилактической работы с учащимися и родителями;

– требования к цифровым компетенциям педагогов в сфере ИБ.

Это подтверждает актуальность настоящего исследования, направленного на теоретическое обоснование и разработку модели проактивного обучения кибербезопасности в школьной практике.

Формирование такой модели позволит восполнить существующий нормативно-методический пробел и предложить педагогически обоснованные решения для развития цифровой грамотности и безопасного поведения учащихся в условиях цифровой трансформации образования.

Эти нормативные документы закладывают фундамент для формирования культуры информационной безопасности и цифровой ответственности на уровне государственных и корпоративных структур.

Однако, проведённый анализ также выявил существенный пробел: в существующей нормативной базе практически отсутствуют документы, напрямую регламентирующие вопросы кибербезопасности в школьной образовательной среде. Ни один из рассмотренных актов не ориентирован на:

– специфику цифровой активности детей и подростков;

– педагогические подходы к формированию киберкомпетентностей;

– обязанности школ, педагогов и родителей в обеспечении кибербезопасной среды;

– механизмов профилактики цифровых рисков в учебной деятельности.

Таким образом, школьное образование остаётся вне рамок прямого регулирования в контексте информационной безопасности,

что затрудняет системную реализацию профилактических и проактивных программ обучения. В условиях, когда учащиеся являются одной из наиболее уязвимых категорий пользователей цифровой среды, данный нормативный вакуум требует пристального внимания со стороны государства и профильных ведомств.

Несмотря на наличие мощной государственной нормативной базы в сфере ИКТ и информационной безопасности, в Казахстане отсутствуют целевые нормативные акты, регламентирующие реализацию кибербезопасности в школах. Это усиливает значимость настоящего исследования, направленного на разработку теоретико-методологических основ проактивного обучения кибербезопасности в средней школе и позволяет рассматривать его как вклад в решение актуальной государственной задачи — обеспечение безопасности цифрового детства в условиях образовательной цифровой трансформации.

## 3.2 Комплекс превентивных стратегий обеспечения кибербезопасности для субъектов образовательного процесса школы

Изучив нормативно–правовую базу Республики Казахстан по направлению кибербезопасности, мы пришли к выводу, что за прошедшие несколько лет в Республике Казахстан выработаны базовые концептуальные подходы к обеспечению и развитию кибербезопасности, которые нормативно закреплены в действующем законодательстве. По поручению Первого Президента Республики Казахстан с 2017 года в стране начата реализация Концепции кибербезопасности «Киберщит Казахстана». Целью Концепции «КИБЕРЩИТ Казахстана» является достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Но обеспечение кибербезопасности школьной образовательной среды однозначно требует разработки и внедрения (или совершенствования) методологической базы, нормативно-правового и организационно-технического обеспечения, политики безопасного использования ИКТ в школьной системе защиты информации и безопасности автоматизированных систем управления, в которых должна быть отражена специфика деятельности школы и оценены все риски кибербезопасности.

Комплекс превентивных стратегий обеспечения кибербезопасности для субъектов образовательного процесса школы представляют собой систему документированных управленческих решений, направленных на защиту определенных защищаемых

процессов и активов в школах, определяют политику кибербезопасности школьной образовательной среды. При разработке данных документов члены рабочей группы ссылались на нормативно–правовые акты Республики Казахстан.

В рамках грантового проекта AP19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента» коллективом Павлодарского педагогического университета имени Әлкей Марғұлан разработан комплекс превентивных стратегий и механизмов противодействия негативному влиянию киберопасности на социальную и психологическую стабильность субъектов образовательного процесса школы. Комплекс превентивных стратегий и механизмов состоит из нескольких документов: концепция воспитательной работы со школьниками как парадигмы кибербезопасности, стандарт обеспечения кибербезопасности образовательной среды школы, методические инструкции обеспечения кибербезопасности образовательной среды школы для учителей, родителей и учеников. Одним из значимых результатов научного поиска в области обеспечения кибербезопасности в школьной среде стало внедрение названных авторских разработок, подготовленных коллективом Павлодарского педагогического университета имени Әлкей Марғұлан в образовательный процесс школ Павлодарской области.

Разработанный комплекс превентивных стратегий и механизмов противодействия негативному влиянию киберопасности на социальную и психологическую стабильность субъектов образовательного процесса школы, состоит из нескольких документов: концепция воспитательной работы со школьниками как парадигмы кибербезопасности, стандарт обеспечения кибербезопасности образовательной среды школы, методические инструкции обеспечения кибербезопасности образовательной среды школы для учителей, родителей и учеников.

Разработанный комплекс превентивных стратегий и механизмов отражает инновационный подход к построению целостной системы кибербезопасности именно в условиях школьного образовательного пространства, восполняя ранее выявленный пробел в национальной нормативной базе, где отсутствуют специализированные регуляторы и методические материалы, направленные на защиту интересов школьников как одной из наиболее уязвимых групп пользователей цифровой среды.

Концепция воспитательной работы со школьниками как парадигмы кибербезопасности (Заседание Ученого совета от 28 марта 2024 г.) направлена на обеспечение единства подходов к мониторингу обеспечения кибербезопасности образовательной среды школы, а также выработку механизмов предупреждения и оперативного реагирования на инциденты кибербезопасности. Она предлагается в

качестве рекомендаций и ориентира для руководителей и педагогов организаций среднего образования по организации воспитательной работы в школе в рамках кибербезопасности. Концепция определяет основные направления воспитательной работы со школьниками в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования цифровых устройств.

Основная цель концепции состоит в том, чтобы дать учащимся, родителям и педагогам школ общие представления о безопасности в информационном обществе, на этой основе сформировать у обучающихся понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности. Концепция включает в себя анализ текущей ситуации, цель и задачи, подходы и принципы воспитательной работы в рамках обеспечения кибербезопасности школьной среды, направления воспитательной работы по повышению у школьников навыков кибербезопасности, мониторинг и оценка и ожидаемые результаты реализации концепции.

В частности, разработанная и утвержденная Концепция воспитательной работы со школьниками как парадигмы кибербезопасности предлагает педагогически обоснованную модель профилактической деятельности в школе, направленную на:

– формирование единства действий педагогов, родителей и администрации по предупреждению киберинцидентов;

– развитие у школьников осознанного и ответственного поведения в цифровом пространстве;

– формирование цифровых компетенций через воспитательные и образовательные мероприятия.

Важным шагом в институционализации подходов к школьной кибербезопасности стало утверждение Стандарта обеспечения кибербезопасности образовательной среды школы, который обеспечивает методологическую связку с национальными и международными требованиями к системе менеджмента информационной безопасности. Этот документ ориентирует школы на выстраивание управляемых процессов оценки и минимизации рисков киберугроз в своей деятельности.

Стандарт обеспечения кибербезопасности образовательной среды школы, который представляет руководство по менеджменту информационной кибербезопасности в организациях среднего образования, поддерживая, в частности, международные и национальные требования к системе менеджмента информационной безопасности в соответствии с законодательством и стандартами Республики Казахстан (от 28 марта 2024 г.). Стандарт включает в себя общие положения, цели и задачи, назначение и область применения, нормативные ссылки, термины и определения, специализированные

компетенции в сфере кибербезопасности, предпосылки создания стандарта, сведения о стандарте, декларация приверженности руководства школы, принципы управления кибербезопасностью, порядок принятия, утверждения и изменения стандарта. В Стандарте отражены основные аспекты управления рисками кибербезопасности.

Дополняют этот комплекс методические инструкции для учителей, родителей и школьников, которые переводят теоретические положения в практические рекомендации по:

– распознаванию угроз и киберинцидентов;

– защите от кибербуллинга и других форм агрессии в сети;

– безопасному использованию цифровых устройств и сервисов.

Методические инструкции содержат материалы по обучению мерам обеспечения кибербезопасности, разъясняют основы кибербезопасности, что нужно знать ребенку, чем опасен Интернет, что такое кибербуллинг и его формы, признаки, указывающие на проблемы в сети ребенка. Также в инструкциях описаны меры как защитить детей от кибербуллинга, рекомендации по кибербезопасности и по техническому контролю.

Разработаны методические инструкции обеспечения кибербезопасности образовательной среды школы для учителей, родителей и учеников. Методические инструкции содержат материалы по обучению мерам обеспечения кибербезопасности, разъясняют основы кибербезопасности, что нужно знать ребенку, чем опасен Интернет, что такое кибербуллинг и его формы, признаки, указывающие на проблемы в сети ребенка. Также в инструкциях описаны меры как защитить детей от кибербуллинга, рекомендации по кибербезопасности и по техническому контролю.

Таким образом, разработанный комплекс не только восполняет нормативно-методический дефицит в сфере школьного киберпространства, но и предлагает практические инструменты проактивного обучения кибербезопасности, направленные на формирование у школьников навыков безопасного поведения и осознанного цифрового гражданства.

Эти материалы могут быть рекомендованы в качестве основы для дальнейшего внедрения в систему школьного образования Республики Казахстан, что делает их значимым вкладом в развитие педагогических и организационно-управленческих механизмов цифровой безопасности в условиях цифровой трансформации общества.

### 3.3 Разработка механизмов противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в школах

Современное информационное школьное сообщество сталкивается с многочисленными угрозами кибербезопасности, которые негативно сказываются не только на технологической, но и на социальной и психологической сферах жизни субъектов образовательной системы. Киберугрозы могут привести к депрессиям, социофобии, недоверию и тревожности. Важно своевременно определить механизмы, которые помогут минимизировать их негативное воздействие.

Сущность системного подхода применительно к изучению проблем психологической кибербезопасности проявляется, прежде всего, в том, что деятельность личности, группы, организации, социума рассматривается как открытая динамическая система в совокупности ее важнейшими внутренними и внешними взаимосвязями для нахождения путей оптимизации этой системы и обеспечения психологической кибербезопасности.

Источником информационной киберопасности при несоблюдении определенных условий могут выступать как внешние, так и внутренние факторы.

Информационно-психологическая кибербезопасность личности – это защищенность жизненно важных интересов личности в информационной сфере, а также осознание личностью негативных информационно-психологических воздействий и освоение механизмов противодействия. Критериями информационно-психологической кибербезопасности на субъективном плане выступают ресурсы личности. Уровень защищенности личности от информационного воздействия зависит от следующих внутренних факторов:

1) форсированность представлений об информационно-психологической кибербезопасности личности: уровневая модель (адекватность представлений способствует сознательному формированию защитных механизмов от информационных угроз);

2) уровень критичности мышления (способность подвергать всестороннему анализу различную информацию с целью выяснения степени ее логичности и эффективности ее применения в данной ситуации); 3) степень внушаемости (субъективная готовность подвергаться и подчиняться информационному воздействию).

Благодаря проведенному исследованию, была поведена классификация уровней сформированности представлений об информационно-психологической кибербезопасности. Выделены основные внутренние ресурсы, субъективные характеристики личности, способствующие ее активизации в сознательном

сопротивлении негативному информационному воздействию, что дает возможность рассмотреть уровни информационно-психологической кибербезопасности, в зависимости от степени проявления этих критериев.

В результате чего обоснована уровневая структурно-функциональная модель информационно - психологической кибербезопасности личности и дано ее детальное описание в условиях разработки механизмов противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в школах.

На современном этапе развития школьного сообщества невозможно опровергнуть тот факт, что одним из важнейших условий развития и нормальной жизнедеятельности личности является беспрерывная информационная связь с окружающим миром. Информационная среда в современном мире развивается стремительно, становясь более разнообразной и насыщенной.

Современные информационные технологии, нормы, установки, ценности, стереотипы поведения обусловлены стремительным развитием компьютерных технологий, глобальным увеличением информационных потоков, усилением угрозы воздействия на сознательные и бессознательные компоненты психики личности на фоне низкого уровня информационной культуры населения (Г.В. Грачев, И.К. Мельник, В.И. Илюхин, В.Н. Лопатин, Г.В. Емельянов и др.). С одной стороны, информация – это мощное средство познания и преобразования как самого человека, так и мира в целом. С другой стороны, информация превращается в серьезную угрозу для безопасности личности.

Как отмечают многие ученые, человек, его повседневная жизнь все больше зависят от массовой коммуникации, которая создает для него своего рода «второю реальность», «субъективную реальность», влияние которой не менее значимо, чем влияние объективной реальности.

Информационно-психологическим фактором риска является информация, оказывающая психотравмирующее, дестабилизирующее влияние на психику человека. Информационное взаимодействие и воздействие в современном мире осуществляется на разных уровнях: государственном, общественном, групповом, личностном.

При этом реципиентом воздействия всегда является личность. Анализ литературы позволяет выделить несколько категорий информационно-психологического воздействия на личность.

Информационный вызов – преднамеренное действие источника информации, направленное на какой-либо социальный объект с открытой или скрытой целью дестабилизации или деформации последнего.

Информационная угроза – реальная опасность информационного воздействия на социальный субъект с целью изменения его потребностей, интересов и ориентации в соответствии с намерениями субъекта информации.

Информационная опасность – реальное информационное воздействие на личность, общество и государство в интересах определенных политических и социальных сил, направленных на дезорганизацию и деформацию устойчивого позитивного развития определенной социальной системы.

В структуре преднамеренного манипулятивного воздействия на личность выделяют: информационно-пропагандистское воздействие – это воздействие словом, информацией с целью формирования определенных взглядов, убеждений.

Психоаналитическое воздействие – это воздействие на подсознание человека. В современном мире практические приемы и техники воздействия на личность становятся все более доступными, практически любой человек без посторонней помощи может изучить их и практиковать в обыденной жизни, используя психологические особенности восприятия.

Знания и учет законов восприятия в процессе информационного воздействия значительно снижает возможности сопротивления личности. Ещё С.Л. Рубинштейн утверждал, что психика соединяет реальное и идеальное и детерминируется двояко: с одной стороны, внутренним фактором, а с другой – она определяется отражаемым, т.е. внешним фактором. Согласно информационному подходу, «Любое явление сознание (как явление субъективной реальности) есть определённая информация, явлённая определённому социальному индивиду». Источником информационной опасности при несоблюдении определенных условий могут выступать как внешние, так и внутренние факторы.

Анализ научной литературы показывает, что внешними факторами опасности могут выступать:

1) полнота, точность, доступность, количество и своевременность поступления информации;

2) соответствие характеристик информационных потоков психологическим возможностям личности (перцептивным параметрам, свойствам психических процессов, установкам личности, поведенческим стереотипам и т.д.);

3) наличие в информационной среде манипулятивных элементов, которые целенаправленно воздействуют как на сознательные, так и бессознательные структуры личности и общества в целом.

Под негативной информацией следует понимать информацию в любой ее форме (текстовая, аудиальная, визуальная, кинестетическая, электронная, графическая), которая причиняет вред физическому, психическому здоровью личности, а также препятствующую

духовному, нравственному развитию. Как отмечает Г.В. Грачев, «Общим источником внешних угроз информационно-психологической безопасности личности является та часть информационной среды общества, которая в силу различных причин не адекватно отражает окружающий человека мир. Т.е. информация, которая вводит людей в заблуждение, в мир иллюзий, не позволяет адекватно воспринимать окружающее и самого себя» [2]. Принципиальной установкой в манипуляции массовым сознанием является предварительное «раскачивание» эмоциональной сферы.

Главным средством для этого служит создание или использование кризиса, антикризисных ситуаций, оказывающей сильное воздействие на чувства.

Менее бурно, но зато более устойчиво проявляются чувства благородные, которые опираются на традиционные положительные ценности. В манипуляции эффективно используется естественное чувство жалости и сочувствия к слабому и беззащитному.

Во многих ситуациях пассивный манипулятор – тот, кто подчеркивает свою слабость, неспособность и даже нежелание управлять оказывается важнейшей фигурой в программе манипуляции. Люди в разной степени подвержены психологическому воздействию. Это связано с возрастными, индивидуально психологическими особенностями личности, жизненным опытом. По мере приобретения жизненного опыта, научных знаний восприимчивость человека к внушению снижается. Однако необходимо отметить, что внушению поддаются все люди, разница только в скорости прививания чужих мыслей и установок.

Критериями информационно-психологической кибербезопасности на субъективном плане выступают ресурсы личности.

Уровень защищенности личности от информационного воздействия зависит от следующих внутренних факторов:

1) сформированность представлений об информационно-психологической безопасности (адекватность представлений способствует сознательному формированию защитных механизмов от информационных угроз);

2) уровень критичности мышления (способность подвергать всестороннему анализу различную информацию, с целью выяснения степени ее логичности и эффективности ее применения в данной ситуации); 3) степень внушаемости (субъективная готовность подвергаться и подчиняться информационному воздействию).

В научной литературе выделяют определенную структуру психологического воздействия на личность: передача определенного объема информации (когнитивный компонент), вызов определенного эмоционального состояния, системы убеждений и мотивов (аффективный компонент), воздействие на бессознательную сферу

личности (суггестивный компонент) и, как следствие, подталкивание к определенному действию (конативный компонент).

Вопрос о критериях информационно-психологической кибербезопасности личности очень сложен, многогранен и неоднозначен из-за двойственности и субъективности данного понятия. То, что кажется информационной угрозой для одной личности, может не соответствовать представлениям другой. Представления – это обобщенные, схематизированные образы, которые формируются на основе многократного восприятия явлений и предметов действительности.

Система представлений является основой взаимодействия человека с объектами действительности, так как индивид должен представить возможные связи и последствия взаимодействия. Сформированность представлений о информационно-психологической кибербезопасности дают личности возможность воспринимать информацию, делать выводы, понимать и придавать смысл и объяснять определенную личностную ситуацию.

Представления тоже включают в себя когнитивный, поведенческий и эмоционально-ценностный компоненты.

Когнитивный компонент включает в себя имеющуюся информацию об информационно-психологической безопасности, ее систематизацию и обобщение.

Поведенческий компонент представлений отражает практические навыки информационного взаимодействия, основанные на жизненном опыте.

Эмоционально-ценностный компонент отражает оценку значимости информационного взаимодействия и его последствий.

Только с появлением смысла в системе «человек – информационная среда» возникает возможность целенаправленной активности личности, возможность перехода из позиции объекта информационного воздействия на позицию субъекта информационного взаимодействия, возможность конструктивной трансформации «картины мира».

Помимо современных научных концепций, у каждого человека складываются субъективные, обыденные представления об информационно - психологической безопасности, которые и играют главную роль в ее практическом обеспечении.

Именно субъективный опыт является регулятором деятельности и мировоззрения. При создании и обосновании уровневой модели информационно-психологической безопасности возникает необходимость классификации сформированности представлений личности об информационно-психологической безопасности

Рассмотрим основные механизмы противодействия негативным последствиям киберопасности.

1. Повышение цифровой грамотности.

Проведение образовательных программ по кибербезопасности является залогом осознанного и безопасного поведения в сети. Знания о фишинге, вредоносном ПО, защите персональных данных позволяют людям эффективнее идентифицировать и предотвращать угрозы. На государственном и корпоративном уровнях важно внедрять обязательные обучающие курсы, семинары и тренинги для различных возрастных групп, начиная со школьников и заканчивая людьми пожилого возраста.

Особое внимание следует уделять развитию критического мышления — умения анализировать получаемую информацию, выявлять потенциально опасные сообщения и сайты, а также понимать основные принципы работы современных интернет-технологий. Важным элементом таких программ должно быть объяснение особенностей социальных сетей, разоблачение схем манипулирования сознанием и разбор примеров психологических атак (social engineering).

Дополнительно следует стимулировать самоконтроль в вопросах управления личными данными, использования надёжных паролей и регулярного обновления программного обеспечения. Вовлечение СМИ в просвещение населения по вопросам кибербезопасности поможет охватить более широкую аудиторию и повысить общий уровень цифровой грамотности населения, а, значит, снизить степень их уязвимости к психологическим и социальным киберугрозам.

2. Разработка и внедрение психологических тренингов.

Регулярные психологические тренинги для школьников, студентов и работников организаций помогут развить стрессоустойчивость, навыки критического мышления и эмоционального реагирования на кибератаки и кибербуллинг. Такие тренинги включают моделирование реальных киберугроз в безопасной среде, что позволяет участникам формировать необходимые поведенческие паттерны и оптимизировать стратегии выхода из стрессовых ситуаций. Особое внимание уделяется развитию способности отличать достоверную информацию от фейковой и обучению методам эффективной коммуникации в случае интернет-угроз. Психологическая поддержка способствует снижению страха и тревожности, связанных с киберпространством, а также формированию устойчивой самооценки, что важно для предотвращения негативных последствий воздействия кибербуллинга и других видов цифровых угроз. В результате, обучающиеся становятся более уверенными пользователями интернета, способными противостоять как техническим, так и психологическим аспектам киберугроз.

Для максимального эффекта эти тренинги рекомендуется проводить в интерактивной форме: с ролевыми играми, групповым обсуждением и работой с кейсами из реальной жизни. Это не только

повышает эффективность обучения, но и способствует развитию командного духа и взаимопомощи при столкновении с киберинцидентами.

3. Правовые меры и государственное регулирование.

Совершенствование законодательства в области кибербезопасности, принятие норм, предусматривающих защиту гражданских прав в цифровом пространстве, а также ужесточение наказаний за киберпреступления способствуют формированию более безопасной среды. Правовые меры и государственное регулирование в области кибербезопасности - это комплекс мер, направленных на защиту информации и информационных систем от киберугроз, основанный на законодательстве и нормативных актах. Они охватывают разработку законов, правил и стандартов, регулирующих отношения в киберпространстве, а также контроль и надзор за их исполнением. Регламент кибербезопасности включает директивы, которые защищают информационные технологии и компьютерные системы с целью заставить компании и организации защищать свои системы и информацию от кибератак, таких как вирусы , черви , троянские кони , фишинг , атаки типа «отказ в обслуживании» (DOS), несанкционированный доступ (кража интеллектуальной собственности или конфиденциальной информации) и атаки на системы управления. В то время как правила кибербезопасности направлены на минимизацию киберрисков и усиление защиты, неопределенность, возникающая из-за частых изменений или новых правил, может существенно повлиять на стратегии реагирования организаций. Существует множество мер по предотвращению кибератак.

4. Технологические решения и инструменты защиты.

Использование антивирусных программ, фильтров контента, инструментов проверки правдивости информации, а также современных систем аутентификации значительно снижает риск воздействия киберугроз. Программы-фильтры (сторожа) представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Антивирусные программы проводят регулярные сканирования файлов на наличие вредоносных программ, обнаруживая и нейтрализуя их перед тем, как они испортят работу компьютера. Они также мониторят активность программ в режиме реального времени, блокируя подозрительные действия и предотвращая возможные атаки на систему.

5. Развитие инфраструктуры оказания психологической помощи онлайн.

Развитие онлайн-психологической помощи подразумевает расширение сети доступных онлайн-сервисов, улучшение их функциональности и повышение квалификации специалистов в сфере

онлайн-консультирования. Создание и поддержка сервисов психологической поддержки, горячих линий и чатов для оперативной помощи жертвам киберугроз может эффективно снизить негативные последствия для психики. Онлайн консультация психолога – это встреча с психологом, которая проходит в онлайн-формате. Вы выбираете себе специалиста, который вам понравился, назначаете «встречу» и связываетесь на любой удобной для вас платформе в любое удобное для вас и для вашего психолога время.

Влияние киберугроз на социальную и психологическую сферы многогранно и требует комплексного подхода к противодействию. Только сочетание образовательных, правовых, технических и психологических мер позволяет снижать масштабы негативного воздействия и формировать устойчивое к современным вызовам информационное общество.

Краткие предложения по теме:

1. Повышение цифровой грамотности способствует осознанному и безопасному поведению в интернете.
2. Психологические тренинги помогают минимизировать стресс и последствия кибербуллинга.
3. Технические средства защиты ограничивают доступ к вредоносному контенту и предотвращают утечку данных.
4. Законодательная поддержка усиливает ответственность за киберпреступления.
5. Оперативная психологическая помощь снижает уровень тревожности и психологического дискомфорта жертв киберугроз.

Смысловой формат гипотез о социальной сущности и структурно-функциональных составляющих психологии кибербезопасности в их эффективности применительно к социальной реальности. И для этого необходимо разработка механизмов противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в школах.

Достижение кибербезопасности исходит из смыслообразующих возможностей субъекта, преодолевающего кризисные или экстремальные информационные ситуации в Сети. Именно личностные образования как «ядро личности» в социально – психологическом направлении можно рассматривать как базовый фактор формирования безопасности.

Инновационный методологический подход требует нового понимания задач и механизмов противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов, которую можно обозначить следующим образом:

- построение целостной теории психологии кибербезопасности на основе всестороннего анализа состояния информационной

безопасности в его социальной представленности, функциональной действенности, мотивационно-потребностный ориентированности, нормативно-ценностной рефлективности.

Политика и обучение основам кибербезопасности ведет к пересмотру модели цифрового обучения. Последовательное обучение избавляет от небезопасных цифровых привычек. Оценив уязвимые места и честно рассказав о них, а затем активно обучая и поощряя безопасные цифровые привычки, учителя превращают учащихся из источника риска в жизненно важную силу.

Формирование культуры кибербезопасности и есть механизмы противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в школах

. Но каждодневная поддержка осведомленности становится еще одним гарантом информационной безопасности школьной среды.

Рассматривается понятие «культура кибербезопасности» в первую очередь предполагает разработку «цифровой школа» как педагогический, дополнительно к технологическому феномену - цифровизации.

Нами предлагаются пути решения задачи о безусловном достижении каждым обучающимся требуемого (зафиксированного в утвержденной образовательной программе) уровня образовательной подготовки на каждой ступени образования в «цифровой школе» вместе с разносторонним развитием его личностного психологического потенциала, использующего возможности цифровой школы. Движение к цифровой школе представляет собой цифровую трансформацию школьного образования на всех его ступенях.

Опыт прошедших десятилетий информатизации школы позволяет сделать следующие выводы:

- цифровые технологии в условиях кибербезопасности - новое явление, и обсуждать их педагогическое и психологическое использование до того, как они станут доступны учебным учреждениям, невозможно;

- чтобы стать эффективным инструментом трансформации образования, они должны быть доступны и освоены в первую очередь педагогами и учебными учреждениями;

- насыщение образовательных организаций средствами цифровых технологий само по себе не ведет к повышению качества их работы;

- появление цифровых технологий должно быть составной частью изменения содержания, методов и организационных форм учебной работы, которые и обеспечивают повышение результативности работы образовательных организаций.

Понятно, что через социальные представления школьники в социальной среде познают и интерпретирует социальную реальность.

Восприятие себя в состоянии кибербезопасности или информационной безопасности обусловливает построение определенных действий и поведения в социуме.

От особенностей конструирования окружающего пространства на современном уровне и от особенностей влияния информации на психологическое восприятия собственного окружения через призму киберопасности/кибербезопасности зависит выстраивание смысложизненных ориентаций, приведение информации о себе в определенную систему, что отражается на самосознании участников школьного сообщества и доминирующих в нем ценностях.

Одна из психологических потребностей детей в школьной среде — потребность в кибербезопасности. Обеспечение информационной безопасности представляет собой такой социальный опыт, который является одним из самых важных для каждого ребенка в школе. Именно потребность в кибербезопасности требует от них в период обучения постоянного переосмысления происходящих социальных событий и поиска адекватных способов преодоления постоянно возникающих угроз как психо - физическому, так и социально - духовному существованию.

Сегодня в целях информационного влияния активно используется сеть Интернет, которая позволяет оказывать целенаправленное воздействие на население страны, отдельные его группы, индивидуумов.

Повышение осведомленности как главный показатель механизмов противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в школах – обучение пользователей.

Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности школьной среды.

Информационно-психологическое воздействие — это такое влияние на индивидуальное или детское сознание, которое вызывает трансформацию психики, а у молодёжи изменение социальных взглядов, мнений, отношений, ценностных ориентаций, мотивов, установок, стереотипов объекта.

Разработка механизмов противодействия негативному влиянию кибербезопасности изучает социо-психологические явления и процессы, возникающие в ситуации угрозы (опасности). Мы рассматриваем структуру социально - психологической стабильности субъектов образовательного процесса в школах в двух аспектах: социальной безопасности школьной среды и психологическая безопасность личности.

С помощью системного подхода описываются механизмы противодействия негативному влиянию кибербезопасности на

социальную психологическую стабильность субъектов образовательного процесса в школах, а также механизмы, определяющие динамику и направленность психического развития.

Среди этих механизмов кибербезопасности важнейшее место занимают две системы — система саморегуляции, самоорганизации деятельности и система структурирования субъектного опыта.

Они определяют активную, целенаправленную и конструктивную позицию школьников в повседневной жизнедеятельности, а также перспективу и основания социально - психологической кибербезопасности личности.

Под социально-психологической кибербезопасностью можно понимать состояние, обусловленное наличием гармоничных, приносящих удовлетворение взаимоотношений (взаимосвязей) личности с другими коммуникаторами, которые позволяют реализовать духовно - психический потенциал личности в процессе жизнедеятельности, сохранить ее целостность. Можно предположить, что основными показателями социально-психологической безопасности являются:

– гармоничный характер взаимодействий и взаимоотношений;

– удовлетворенность межличностными отношениями;

– чувство защищенности от негативных психологических воздействий (унижений, оскорблений, киберугроз, принуждений, игнорирования, манипулирования и т.п.) со стороны партнеров по взаимодействию в сети интернет;

– отсутствие напряженности, трудностей, нарушений в отношениях (в том числе в общении).

Ключевыми понятиями становятся межличностные отношения и коммуникация учащихся в школьной среде. При этом в контексте социально-психологической кибербезопасности межличностные отношения должны рассматриваться с точки зрения отсутствия трудностей, нарушений, деформаций (т.е. снижением затруднений в общении), характеризоваться наличием гармоничности и удовлетворенности отношениями у субъектов.

В данном случае речь идет о проблеме локализации психологического барьера или, другими словами, о проблеме поиска «носителя» затрудненности общения. В этом отношении приведенное определение довольно показательно, поскольку, кроме сведений о функциях психологического барьера (сокрытие эмоционально-интеллектуального потенциала активности), оно содержит прямое указание и на основного его «носителя» (личность) и выделяет формы (способы) существования психологического барьера (процессы, свойства, состояния человека в целом).

Эмоционально-интеллектуальный потенциал активности в сфере цифровой грамотности – механизм механизмов противодействия

негативному влиянию кибербезопасности на социальную психологическую стабильность

1. Когнитивная сфера. Способность оперировать гипотезами при решении интеллектуальных задач и способность анализировать абстрактные идеи, искать ошибки и логические противоречия в абстрактных суждениях - всем этим должен обладать взрослый человек.

2. Эмоционально-мотивационная сфера. Развитие и коррекция эмоционально-мотивационной сфер личности, особенно личности студента, характеризуется некоторой спецификой. У молодых людей на первое место выдвигаются мотивы, связанные с жизненным планом личности, ее намерениями в профессиональном становлении, ее мировоззрением.

3. Поведенческая сфера. Для детей любой возрастной и социальной группы, общение - важная доминанта жизнедеятельности. Установление социальных контактов: личностных и эмоциональных зависит от коммуникативных способностей, его коммуникативной компетентности. Во многом, именно от того, как будет развита система межличностных отношений, зависит социально-психологическая кибербезопасность личности.

В результате возникает огромная проблема: как подготовить субъектов образования жить в мире цифрового пространства, как сформировать у него информационную грамотность, базовые навыки искать, проверять, отбирать, анализировать, хранить информацию, как научиться всему этому, не запутаться в многообразии информационных потоков, отличить важную информацию от неважной, лживую от истинной, как оценить достоверность информации.

Достоверность определяется с точки зрения полноты, целостности и истинности информации. При этом последнему фактору уделяется основное внимание.

Достоверность определенной информации важно отследить согласно общим принципы достоверности полученной информации: полный, целостность, истинность.

Поэтому при обучении организации процесса поиска следует уделять особое внимание всем трем составляющим, определяющим качество полученных данных.

Полнота информации может быть решена, в том числе, за счет грамотного планирования поискового запроса.

Целостность информации, представленной на страницах сайта, во многом зависит от корректности ее сохранения и сочетания форм представления с возможностями используемого браузера.

Истинность информации.

Наиболее высок и важен тот, кто умеет определять, — это полученная им информация от Истины. От этого, в местном счете, будет зависеть достоверность полученной информации.

Определение обоснованности и точности информации является довольно простым для пользователя.

Контроль достоверности информации в социальных сетях в настоящее время является весьма актуальной задачей, поскольку все больше детей становится активными их пользователями, и при этом количество угроз постоянно возрастает.

Сегодня ответственность за проверку того, насколько правдива представленная в социальной сети информация, ложится на плечи каждого пользователя, заинтересованного в получении достоверной информации.

Однако ручной анализ, при котором необходимо оценить репутацию ресурса и автора и совершить перекрестную проверку данных в различных источниках, отнимает много времени и сил, кроме того, он требует от пользователя беспристрастности.

Реализация предложенного подхода позволит упростить эту проверку. Разработанный метод противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов как механизм должен быть достаточно универсальным для того, чтобы его можно было применять в любой социальной сети.

Возможно два варианта его использования.

Беспристрастность – это качество, которое часто прославляется как одно из высших в человеческой природе. Она выражает способность рассматривать ситуации и проблемы без предвзятости или субъективных предубеждений. Беспристрастность позволяет нам принимать обдуманные решения и поступки, основанные на объективном взгляде на мир. В этом тексте мы рассмотрим суть и принципы беспристрастности, а также ее значение для личного развития и социальной гармонии. Другим важным аспектом проявления беспристрастности в детях является способность рассматривать различные точки зрения на проблему или ситуацию

Ключевые аспекты беспристрастности как формы психологической цифровой грамотности: механизм противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность

*1. Беспристрастность это - нейтралитет. Воспитать детей беспристрастными означает, что они активно будут действовать справедливо, а не просто оставаться вне драки.*

*2. Беспристрастность требует готовности признать и противостоять собственным предубеждениям и быть полностью объективным или нейтральным.*

*3. Беспристрастность означает готовность признать проблемы преодоления:*

*- поиск разнообразных перспектив, оспаривание собственных предположений и открытие для новых идей.*

*3. Беспристрастность требует от субъекта образования принятия трудных решений, которые могут понять кибербуллинг и критически рассмотреть свои негативные реакции.*

В разработке механизмов противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в образовательной сфере большую роль играет система социально - психологических ценностей.

Это система мер – механизмов, защищающих школьников от травмирующей, этически некорректной, незаконной информации и защитить от кибербуллинга, груминга и секстинга.

Кибербуллинг — это травля с использованием цифровых технологий. Кибербуллинг может происходить в социальных сетях, мессенджерах, на игровых платформах и в мобильных телефонах. Это целенаправленная модель поведения, которая ставит своей задачей запугать, разозлить или опозорить того, кто стал объектом травли.

Груминг (от английского: grooming) — процесс создания доверительных отношений с ребёнком или подростком (также иногда и с его близкими) с целью последующей сексуальной эксплуатации. Это одна из форм сексуализированного насилия над детьми через создание эмоционально теплых, хороших отношений.

«Секстинг» — это отправка и получение фотографий, сообщений и видео откровенно сексуального характера с помощью текстовых сообщений, электронной почты или размещения в социальных сетях.

Цифровая грамотность в аспекте защиты от кибербуллинга заключается в формирование навыков самозащиты:

- не выкладывать личные данные: адреса, фотографии, телефоны, почты и тем более - пароли от почт или личных кабинетов. ...
- не общаться с незнакомцами. ...
- не высказываться негативно о других в виртуальной среде. ...
- игнорировать агрессию и угрозы.

В целях защиты необходимо применять так же нормы закона «О защите прав ребенка», определяющие его права на защиту от сведений, которые могут причинить моральную и психологическую травму. Необходимо создавать перечни документов, программ и иных источников, которые могут защитить психику и социальную среду детей.

Это станет одной из основ информационной безопасности.

Основной целью школьной кибербезопасности является предотвращение компрометации информации.

Необходим комплекс мероприятий по информированию субъектов образования о методах и способах их обмана, а также системе образования уделить внимание и диагносцировать, в каких противоправных действиях участвуют сами подростки и что грозит за незаконный бизнес в интернете.

Цифровая гигиена в онлайн-играх как формы социальной цифровой грамотности механизм противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность

Цифровая грамотность социальной среде школьников — умение положительно взаимодействовать с современными цифровыми инструментами:

- пользоваться сайтами и приложениями;
- генерировать контент;
- в целом уверенно пользоваться существующими технологиями.

Разработка механизмов противодействия негативному влиянию кибербезопасности вопрос в том, что известно учащимся о правилах безопасного поведения в соцсетях и мессенджерах, есть ли знания о цифровой гигиене в онлайн-играх.

Важную роль в достижении этой цели играет триада безопасной IT-инфраструктуры — конфиденциальность, целостность и доступность. Под конфиденциальностью в данном контексте подразумевается набор правил, ограничивающих доступ к информации.

Целостность взаимодействия гарантирует понимание, что информация является точной и достоверной или ложной. Доступность, в свою очередь, отвечает за надежность доступа к информации уполномоченных лиц. Совместное рассмотрение принципов триады помогает компаниям разрабатывать политики безопасности, обеспечивающие надежную защиту.

Кибергигиена как способ противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в школах:

– это полезные привычки при работе в интернете, которые необходимо вырабатывать для того, чтобы не попадаться на уловки киберпреступников. При приобретении необходимых навыков пользователь, выполняя свои действия в Сети, будет чувствовать себя уверенно и защищенно в Сети.

Кибергигиена в школьной среде нацелена на сохранность и безопасность субъектов образования, оборудования и ПО, защиту от различного рода вредоносных действий киберпреступников.

Соблюдение и поддержание должного уровня кибергигиены в школьно организации помогает сохранять и в домашних условиях исключить нарушения в области безопасности и сохранить в неприкосновенности личные и конфиденциальные данные.

Однако для того, чтобы полезные привычки закрепились и стали частью поведения детей, требуется постоянная практика.

Как обеспечить соблюдение кибергигиены?

- Регулярные действия и привычки
- Использование надлежащих инструментов
- Хранение паролей в безопасности
- Использование многофакторной аутентификации
- Регулярное резервное копирование данных
- Обеспечение конфиденциальности
- Обновление приложений, программного обеспечения и прошивок

Именно благодаря развитию у пользователей навыков кибергигиены возможно снизить количество киберинцидентов.

Кибергигиена еще и есть способность К Анализу Собственных Эмоций и Предубеждений

Этот способ позволит субъектом образования развить способность к анализу и осознанию своих собственных эмоций и ситуации и проблем с объективной точки зрения, не допуская влияния субъективных предпочтений или эмоций. Это дает возможность отличается способностью принимать решения на основе фактов и логики, а не исключительно на основе личных предубеждений, и чтобы их решения были сбалансированными и обоснованными.

В разработку механизмов противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность субъектов образовательного процесса в школах входит набор документов:

Право на доступ к информации может быть ограничено только законами и лишь в той мере, в какой это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения.

Закон Республики Казахстан от 21 мая 2013 года 94-V «Закон о персональных данных и защите информации»; Кодекс Республики Казахстан от 18 сентября 2009 года № 193-IV «О здоровье народа и системе здравоохранения» с изменениями от 15 апреля 2013 года; СТ РК ИСО/МЭК 27002-2009 - Информационные технологии.

Закон Республики Казахстан «О доступе к информации» от 16 ноября 2015 года № 401-V ЗРК. 3. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

В соответствии со ст. 1 Закона РК «О персональных данных и их защите» (далее - Закон) персональные данные - это сведения, относящиеся к определенному или определяемому на их основании

субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

Служба социально-психологической кибербезопасности личности механизм противодействия негативному влиянию кибербезопасности на социальную психологическую стабильность

Одной из основных целей подобной службы социально-психологической кибербезопасности личности может стать проведение просветительской работы с целью повышения психологического отношения к сети интернет, формирования защищенности и понимание психологической и социальной устойчивости (психологической) помощи.

Задачами службы социально-психологической кибербезопасности личности учащихся являются:

– изучение индивидуально-психологических особенностей личности: когнитивных процессов, эмоциональной и мотивационной сферы, сферы межличностных отношений (особенностей поведения в межличностных отношениях).

Изучение особенностей развития и становления личности. Выявление причин и механизмов нарушений в обучении, развитии, социальной адаптации;

– профилактика и меры по преодолению отклонений в социальном и психологическом здоровье, а также в развитии личности;

– содействие в приобретении психологических знаний, умений, навыков, необходимых для общего развития, достижения успеха в жизни в целом, повышения уровня защищенности (социально-психологической безопасности);

– проведение психологических исследований в области социального развития личности, групповых взаимодействий. Поиск эффективных методов социально-психологического воздействия.

Реализация поставленных задач может осуществляться в двух формах: индивидуальной и групповой.

Индивидуальная работа (психодиагностика и психокоррекция) проводится, прежде всего, с целью выявления причин и механизмов нарушений и деформаций в развитии, социальной адаптации; а также с целью разрешения проблем и внутриличностных конфликтов, затрудняющих развитие и становление личности.

Групповые формы работы проводятся с целью профилактики отклонений в социальном и психологическом здоровье личности, помощи в стабилизации их эмоционального состояния и межличностных отношений, а также направлены на содействие в приобретении личностью психологических знаний, умений, навыков, необходимых для общего и профессионального развития.

На фоне развития отдельных компонентов происходит формирование Я-концепции личности, самосознания, мировоззрения,

что является центральным звеном развития и становления личности. Самосознание и мировоззрение человека являются определяющими для социально-психологической безопасности личности. Чем более целостной и сбалансированной является личность, тем более устойчивой к негативным воздействиям и переживаниям она будет, тем более высокой будет ее социально-психологическая безопасность.

# ЗАКЛЮЧЕНИЕ

В условиях цифровизации образовательного пространства обеспечение кибербезопасности становится важнейшим направлением развития системы образования. Школьная среда как часть единого информационного пространства подвержена многочисленным рискам: от несанкционированного доступа к персональным данным до деструктивного влияния интернет-контента на психику обучающихся. Эти вызовы требуют не только технических решений, но и педагогических подходов, ориентированных на формирование цифровой культуры, развитие критического мышления и навыков безопасного поведения в интернете.

В рамках данной монографии представлено теоретическое обоснование и практическая модель педагогического обеспечения кибербезопасности в школе, основанная на принципах комплаенс-менеджмента. Комплаенс-подход позволяет выстроить систему профилактики цифровых угроз через формализацию правил, норм и алгоритмов поведения в цифровой среде, вовлекая в этот процесс всех участников образования — администрацию, педагогов, родителей и самих обучающихся.

В ходе исследования были:

– проанализированы ключевые понятия и нормативно-правовая база в сфере кибербезопасности и образования;

– выявлены риски и уязвимости цифровой школьной среды;

– разработана модель педагогического сопровождения с включением ценностного, содержательного и процессуального компонентов;

– апробированы цифровые ресурсы и методические материалы на базе школ, подтверждающие эффективность предложенного подхода.

Научная и практическая значимость работы заключается в том, что представленная модель может быть масштабирована и адаптирована под условия конкретного образовательного учреждения. Она способствует не только профилактике цифровых угроз, но и формированию устойчивой культуры кибербезопасности у подрастающего поколения, что особенно актуально в условиях непрерывного цифрового развития общества.

Внедрение описанного в монографии подхода может стать важным шагом к построению целостной и безопасной образовательной среды, в которой обучение и воспитание происходят с учётом современных вызовов и стандартов информационной безопасности.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ


1. Kern D., Bean R.M. ILA 2017 standards: Key notions, challenges, and opportunities for middle and high school classroom teachers//Journal of Adolescent & Adult Literacy. - 2018. Vol. 62. No. 1. – pp. 89–94. https://doi. org/10.1002/jaal.875.
2. Pyżalski J. From cyberbullying to electronic aggression: Typology of the phenomenon//Emotional and Behavioural Difficulties. - 2012. - Vol. 17. No. 3–4. – pp. 305–317. https://doi.org/10.1080/13632752.2012.704319.
3. Kopecký K. Czech children and Facebook– A quantitative survey//Telematics and Informatics. - 2016). Vol. 33. No. 4. – pp. 950–958. https://doi.org/10.1016/j.tele.2016.02.008.
4. Fineberg, N., Demetrovics Z., Stein D., Ioannidis K., Potenza M., Grünblatt E. Manifesto for a European research network into problematic usage of the internet//European Neuropsychopharmacology. - 2018. https://doi.org/10.1016/j.euroneuro.2018.08.004.
5. Walotek-Ściańska K., Szyszka M., Wąsiński A., Smołucha D. New media in the social spaces. Strategies of influence//Verbum: Prague. - 2014.
6. Szpunar M. Imperializm kulturowy Internetu. Kraków: Wydawnictwo UJ. - 2017.
7. Tomczyk Ł. Digital piracy among adolescents — scale and conditions//In Proceedings New Trends And Research Challenges In Pedagogy and Andragogy Ntrcpa18. - 2018. https://doi.org/10.24917/9788394156893.5.
8. Livingstone S. The class: Living and learning in the digital era//Comunicação & Educação. - 2018. Vol. 23. No. 1. – p. 127. https://doi.org/10.11606/issn.2316-9125.v23i1p127-139.
9. Livingstone S., Mascheroni G., Staksrud E. European research on children's internet use: Assessing the past and anticipating the future//New Media & Society. - 2017. Vol. 20. No. 3. – pp. 1103–1122. https://doi. org/10.1177/1461444816685930.
10. Pyżalski J., Zdrodowska A., Tomczyk Ł., Abramczuk K. Polskie badania EU KIDS ONLINE//Najważniejsze wyniki i wnioski.Poznań: Wydaw. Uniwersytet Adama Mickiewicza. - 2019.
11. Neumann C. Teaching digital natives: Promoting information literacy and addressing instructional challenges//Reading Improvement. - 2016. Vol. 53. No. 3. – pp. 101–106.
12. Velickovic S., Stosic L. Preparedness of educators to implement modern information technologies in their work with preschool children//International Journal of Cognitive Research in Science. Engineering and Education. - 2016. – Vol. 4. No. 1. – pp. 23–30. https://doi.org/10.5937/ijcrsee1601023v.

13. Bayraktar F. Online risks and parental mediation strategies comparison of Turkish children/ adolescents who live in Turkey and Europe//TED EĞİTİMVEBİLİM. - 2017. https://doi.org/10.15390/eb.2017.6323.

14. Tomczyk Ł., Wąsiński A. Parents in the process of educational impact in the area of the use of new media by children and teenagers in the family environment//TED EĞİTİMVEBİLİM. - 2017. https://doi. org/10.15390/eb.2017.4674.

15. Hobbs R., Tuzel S. Teacher motivations for digital and media literacy: An examination of Turkish educators//British Journal of Educational Technology. - 2017. Vol. 48. No. 1. – pp. 7–22. https://doi.org/10.1111/bjet.12326.

16. Preradović N.M., Lešin G., Boras D. The role and attitudes of kindergarten educators in ICT supported early childhood education//TEM Journal. - 2017. Vol. 6. No. 1. – pp. 162–172. https://doi.org/10.18421/TEM61-24.

17. Eger L., Klement M., Tomczyk Ł., Pisoňová M., Petrová G. Different user groups of university students and their ICT competence: Evidence from three countries in Central Europe//Journal of Baltic Science Education. - 2018. – Vol. 17, No. 5.

18. Hobbs R., Coiro J. Design features of a professional development program in digital literacy//JournalofAdolescent&AdultLiteracy. - 2019. – Vol. 62. No. 4. – pp. 401–409. https://doi.org/10.1002/jaal.907.

19. Eyal L. Digital assessment literacy– the core role of the teacher in a digital environment//Journal of Educational Technology & Society. - 2012. Vol. 15. No. 2. – pp. 37–49.

20. Yusupova N.G., Skudareva G.N. New resource solutions in the development of future teacher digital literacy//Astra Salvensis. - . (2018). - pp. 261–270.

21. Lindstrom D. L., Niederhauser D. S. Digital literacies go to school: A cross-case analysis of the literacy practices used in a classroom-based social network site//Computers in the Schools. - 2016. Vol. 33. No. 2. – pp. 103-119. https://doi.org/10.1080/07380569.2016.1179025.

22. Potyrała K. iEdukacja. In Synergia nowych mediów i dydaktyki. Kraków: Wydawnictwo Uniwersytetu Pedagogicznego. - 2017.

23. Lamanauskas V. Reflections on education. Siauliai: Scienta Socialis. - 2017.

24. Al-Qallaf C.L., Al-Mutairi A.S.R. Digital literacy and digital content supports learning. Electronic Library. - 2016. Vol. 34. No. 3). – pp. 522–547. https://doi.org/10.1108/EL-05-2015-0076.

25. Mendoza A. Preparing preservice educators to teach critical, place-based literacies//Journal of Adolescent & Adult Literacy. - 2018. Vol. 61. No. 4. – pp. 413–420. https://doi.org/10.1002/jaal.708.

26. Stošić L., Stošić I. Perceptions of teachers regarding the implementation of the internet in education//Computers in Human

Behavior. - 2015. Vol. 53. - Pp. 462–468. https://doi.org/10.1016/j.chb.2015.07.027.

27. Livingstone S., Haddon L. EU Kids Online. Zeitschrift Für Psychologie// Journal of Psychology. - 2009. – Vol. 217. No. 4. – pp. 236–239. https://doi.org/10.1027/0044-3409.217.4.236.

28. Fantin M. Perspectives on media literacy, digital literacy and information literacy//International Journal of Digital Literacy and Digital Competence. - 2010. Vol. 1. No. 4. – pp. 10–15. https://doi.org/10.4018 /jdldc.2010100102.

29. Kajee L. Digital literacy: a critical framework for digital literacy practices in classrooms.//EDULEARN16 Proceedings. - 2016. https://doi.org/10.21125/edulearn.2016.0374.

30. Lohnes Watulak S. Reflection in action: Using inquiry groups to explore critical digital literacy with pre-service teachers//Educational Action Research. - 2016. – Vol. 24. No. 4. – pp. 503–518. https://doi.org/10.1080 /09650792.2015.1106957.

31. Berge O. Rethinking digital literacy in Nordic school curricula//Nordic Journal of Digital Literacy. - 2017. Vol. 12. No. 01–02. – pp. 5–7. https://doi.org/10.18261/issn.1891-943x-2017-01-02-01.

32. van de Oudeweetering K., Voogt J. Teachers' conceptualization and enactment of twenty-first century competences: Exploring dimensions for new curricula//Curriculum Journal. - 2018. Vol. 29. No. 1. – pp. 116–133. https://doi.org/10.1080/09585176.2017.1369136.

33. Potter J. Framing the terms and conditions of digital life: New ways to view "known" practices and digital/media literacy//Learning, Media and Technology. - 2017. Vol. 42. No. 4. – pp. 387–389. https://doi.org/10.1080 /17439884.2017.1397019.

34. Bazalgette C., Buckingham D. Literacy, media and multimodality: A critical response//Literacy. - 2013. Vol. 47. No. 2. – pp. 95–102. https://doi.org/10.1111/j.1741-4369.2012.00666.x.

35. Harbaugh R., Khemka R. Does copyright enforcement encourage piracy?*.// The Journal of Industrial Economics. - 2010. Vol. 58. No. 2. – pp. 306–323. https://doi.org/10.1111/j.1467-6451.2010.00419.x.

36. Lee S.-H. Digital literacy education for the development of digital literacy// International Journal of Digital Literacy and Digital Competence. - 2014. Vol. 5. No. 3. – pp. 29–43. https://doi.org/10.4018/ijdldc.2014070103.

37. Tomczyk Ł., Szotkowski R., Fabiś A.,Wąsiński A., Chudý Š., Neumeister P. Selected aspects of conditions in the use of new media as an important part of the training of teachers in the Czech Republic and Poland- differences, risks and threats//Education and Information Technologies. - 2015. Vol. 22. No. 3. – pp. 747–767. https://doi.org/10.1007/s10639-015-9455-8.

38. Teo T., Chai C. S., Hong H.-Y. Singaporean and Taiwanese pre-service teachers' beliefs and their attitude towards ICT use: A comparative

study//The Asia-Pacific Education Researcher. - 2009. Vol. 18. No. - 1. https://doi. org/10.3860/taper.v18i1.1040.

39. Khokhar A. Why do teachers educators not practice what they believe: ict integration gaps//ICERI2016 Proceedings. - 2016. https://doi.org/10.21125/iceri.2016.0556.

40. Wyżga O., Mróz A. Polish teachers in changing reality//Sino-US English Teaching. – 2018. Vol. 15. No. 6. https://doi.org/10.17265/1539-8072/2018.06.003.

41. Macuch B., Raspor A., Sraka M., Kovačič A. Media exposure and education of first to six grade children from Slovenia- parent opinions//International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE). - 2018. Vol. 6. No. 3. – pp. 49–57. https://doi.org/10.5937/ijcrsee1803049M.

42. Borthwick A. C., Hansen R. Digital literacy in teacher education: Are teacher educators competent?//Journal of Digital Learning in Teacher Education. - (017. Vol. 33. No. 2. – pp. 46–48. https://doi.org/10.1080 /21532974.2017.1291249.

43. Veteska J. Uvod do teorie zdelavani dospelych a andragogiky//Usti nad Labem: Univerzita J. Purkyne. - 2017.

44. Баранов А.А. Информационная безопасность: учебник для вузов. – М.: Юрайт, 2021. – 356 с.

45. Гришина Н.В. Кибербезопасность: учебное пособие. – СПб.: Питер, 2020. – 272 с.

46. Жданов И.А. Основы кибербезопасности: учебное пособие. – М.: КНОРУС, 2019. – 248 с.

47. Информационная безопасность: учебник / под ред. С.Г. Симонова. – М.: Академия, 2022. – 512 с.

48. Карпов В.Н. Технологии защиты информации: учебник для бакалавров. – М.: Инфра-М, 2021. – 384 с.

49. Касперский Е.В. Компьютерные вирусы и киберугрозы: практческое руководство. – М.: Эскимо, 2020. – 320 с.

50. Михайлов С.А. Информационная безопасность и защита информации в компьютерных системах: учебное пособие. – Казань: Казанский университет, 2019. – 210 с.

51. Соловьев А.А. Кибербезопасность и киберугрозы: монография. – Новосибирск: Наука, 2021. – 290 с.

52. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2017. - №31. – Ст. 4736.

53. Национальный стандарт Российской Федерации ГОСТ Р 57580. 1 – 2017. Защита информации финансовых организации. – М.: Стандартинформ, 2018. – 45 с.

54. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. – Gaithersburg, MD:

NIST, 2018. – 55 p.

55. Von Solms R.,Van Niekerk J. From information security to cyber security. – Computers & Security. – 2013. – Vol. 38. – P. 97-102.

56. Stallings, W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. – Boston: Addison-Wesley, 2019. – 840 p.

57. Вятлева О.А., Курганский А.М. Режимы пользования мобильным телефоном и здоровье детей школьного возраста // Гигиена и санитария. 2019. Т. 98. № 8. С. 857-862.

58. Тихон А. Влияние мобильных телефонов на здоровье человека // Medicus. 2019. № 4 (28). С. 19-27.

59. Бруев И.А. Влияние мобильных телефонов на психическое и физическое здоровье студентов (номо-фобия) // Научные известия. 2022. № 27. С. 58-60.

60. Лежнина Л.В., Егошина Е.Д. Интернет-зависимость и депрессия у студентов // Герценовские чтения: психологические исследования в образовании. 2021. № 4. С. 342-349.

61. Сулакшин С.С. Нравственность российского общества и факторы влияния (интернет, телевидение) // Политика и общество. 2014. № 9 (117). С. 1065-1081.

62. Цой Н.А. Социальные факторы феномена интернет-зависимости: специальность 22.00.04 «Социальная структура, социальные институты и процессы»: Дис. ... кандидата социологических наук. Владивосток, 2011. 206 с.

63. Зверянская Л.П. Интернет-зависимость как основная причина развития киберпреступности // Фундаментальные и прикладные исследования: проблемы и результаты. 2015. № 17. С. 239-243.

64. Герни Дж. Цифровая грамотность «так же важна, как чтение и письмо» [Электронный ресурс]. – URL: https://surl.lu/keursg (дата обращения: 07.09.2025).

65. Belshaw D. What is ‘digital literacy’? A Pragmatic Investigation: PhD Thesis. – Durham: Durham University, 2011. – 350 p.

66. Wawra D. Linguistic Literacy and Political Communication in the Digital Age [Электронный ресурс]. – URL: https://blogs.ubc.ca/oer.pressbooks.pub (дата обращения: 07.09.2025).

67. Wawra D. ‘Managing Migration:’ Diskurse von EU-Institutionen und US-Regierung zur Migration. Eine kritische Analyse / In: Hansen C., Ricart-Brede J. (Hrsg.). Migration, das finde ich …: Multidisziplinäre Perspektiven auf ein allgegenwärtiges Phänomen. – Göttingen: Vandenhoeck & Ruprecht unipress, 2023. – S. 91–115.

68. Бочарова М. Безопасно в Интернете. Better Internet for Kids / ЮНИСЕФ [Электронный ресурс]. – URL: https://www.betterinternetforkids.eu (дата обращения: 07.09.2025).

69. Gilster P. Digital Literacy. – New York: Wiley, 1997. – 240 p.

70. Hargittai E. Survey measures of web-oriented digital literacy // Social Science Computer Review. – 2005. – Vol. 23, № 3. – P. 371–379.

71. Берман Н.Д. К вопросу о цифровой грамотности // Современные исследования социальных проблем. – 2018. – Т. 10, № 3. – С. 34–42.

72. Государственная программа «Цифровой Казахстан». – Астана, 2017. – 97 с.

73. Гайсина С. В. Цифровая грамотность и цифровая образовательная среда школы //Методические рекомендации. – 2018. – С. 5.

74. Что такое уязвимость безопасности? [Электронный ресурс]. – URL: https://www.csoonline.com/article/security-vulnerability (дата обращения: 07.09.2025).

75. Шариков А. В. Подходы к концептуализации цифровой грамотности // Вестник Московского университета. Серия 10: Журналистика. – 2019. – № 5. – С. 25–39.

76. Лоевус Л. Что такое цифровая грамотность? / Education Week [Электронный ресурс]. – URL: https://www.edweek.org (дата обращения: 07.09.2025).

77. Уязвимость (компьютерная безопасность) [Электронный ресурс]. – URL:

78. Семёнова И. С. Цифровая культура как социальный феномен [Электронный ресурс]. Semantic Scholar. – URL: https://www.semanticscholar.org (дата обращения: 07.09.2025).

79. Хашеми-Пур К. Что такое триада ЦРУ (конфиденциальность, целостность и доступность)? [Электронный ресурс]. – URL: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA (дата обращения: 07.09.2025).

80. https://ru.wikipedia.org/wiki/Уязвимость_(компьютерная_безопасность) (дата обращения: 07.09.2025).

81. 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.

82. 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.

83. 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.

84. 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.

85. 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.

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

87. 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/.

88. 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.

89. 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.

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

91. 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.

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

93. D'Andrea, A., Ferri, F., Grifoni, P. An overview of methods for virtual social networks analysis // Computational Social Network Analysis: Trends, Tools and Research Advances. Springer, 2009, pp. 3–25.

94. 2.2.2 Chou, C., Condron, L., Belland, J. C. A review of the research on Internet addiction // Educational Psychology Review. 2005, vol. 17, pp. 363–388.

95. Huesmann, L. R., Taylor, L. D. The role of media violence in violent behavior // Annual Review of Public Health. 2006, vol. 27, no. 1, pp. 393–415.

96. Концепция кибербезопасности «Киберщит Казахстана». Утверждена Правительством Республики Казахстан, июнь 2017 года.

97. Закон Республики Казахстан «О защите детей от информации, причиняющей вред их здоровью и развитию». Принят 2 июля 2018 года, статья 4.

98. Zhilbayev, Z. O. Комплаенс-менеджмент и управление рисками кибербезопасности в системе школьного образования: теоретический обзор // Bulletin of the Karaganda University. Pedagogy

series. 2024, № 1 (11329), pp. 106–113.

99. ISO/IEC 27001:2022 – Information Security Management Systems — Requirements. Международный стандарт, опубликован в октябре 2022 года.
NIST Cybersecurity Framework. Framework for improving critical infrastructure cybersecurity, NIST.
COBIT. Control Objectives for Information and Related Technologies, ISACA, актуальная версия — COBIT 2019.

100. Стандарт обеспечения кибербезопасности образовательной среды школы. Разработан рабочей группой проекта AP19678646 Маргулан Университета.

101. Положение о кибербезопасности школы. Разработано в рамках проекта AP19678646 Маргулан Университета.

102. Методические инструкции по КБ - Разработаны рабочей группой проекта AP19678646 Маргулан Университета.

103. Syrymbetova, L. S. et al. Parameters and criteria of the school educational environment expertise // Pedagogy and Psychology. 2023, vol. 56, no. 3, pp. 124–130.a

104. International Organization for Standardization. (2018). ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. Geneva: ISO. URL: https://www.iso.org/standard/75281.html.

105. Martin, F., Bacak, J., Byker, E. J., Wang, W., Wagner, J., & Ahlgrim-Delzell, L. (2023). Examination of Cybersecurity Technologies, Practices, Challenges, and Wish List in K-12 School Districts.Journal of Cybersecurity Education, Research & Practice. https://doi.org/10.32727/8.2023.9.

106. Obioha-Val, O. (2024). The Role of Artificial Intelligence (AI) in Enhancing Cybersecurity for Educational Technologies in US Public Schools.Asian Journal of Research in Computer Science. https://doi.org/10.9734/ajrcos/2024/v17i11523.

107. Beneš, M. (2024). Kyberbezpečnost jak součást digitální gramotnosti: Jak mohou školy vytvářet podpůrné a bezpečné prostředí z hlediska kybernetické bezpečnosti.Gramotnost, Pregramotnost a Vzdělávání. https://doi.org/10.14712/25337890.4734.

108. Krupa, C. R., Kavitha, R., Vasundhra, G., & Kavidharshini, I. (2024).Safeguarding Digital Learning Environments in the Era of Advanced Technologies. https://doi.org/10.1201/9781032711300-16.

109. Román, N. J. P., & Martínez, L. A. M. (2024). Ciberseguridad enfocada en el futuro digital de los estudiantes.LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades. https://doi.org/10.56712/latam.v5i2.1910.

110. Chen, I., & Shen, L. (2016).The Cyberethics, Cybersafety, and Cybersecurity at Schools. https://doi.org/10.4018/IJCEE.2016010101.

111. Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller,

R. E. (2020). Planning for Cyber Security in Schools: The Human Factor.Educational Planning.

112. Arishia, A. A., Kamarudinb, N. H., Bakarc, K. A. A., Shukurd, Z. B., & Hasan, M. K. (2024). Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences.International Journal of Advanced Computer Science and Applications. https://doi.org/10.14569/ijacsa.2024.0151249.

113. Национальный стандарт РК «СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования».

114. Закон Республики Казахстан от 24.11.2015 г. «Об информатизации».

115. Закон Республики Казахстан от 05.07.2004 г. «О связи».

116. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 — 2029 годы».

117. Постановление Правительства Республики Казахстан от 20.12.2016 г. № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

118. Постановление Правительства Республики Казахстан от 09.08.2018 г. № 488 «Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности».