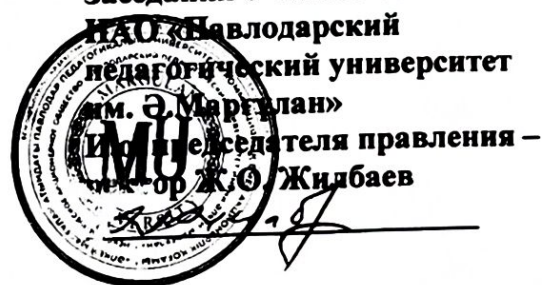


Министерство науки и высшего образования Республики Казахстан
НАО «Павлодарский педагогический университет им. Ә.Марғұлан»

Утверждено
Решением Ученого совета
(Протокол №6 от 28.02.2028 г.
Заседания Ученого совета



КОНЦЕПЦИЯ
воспитательной работы со школьниками как парадигмы
кибербезопасности

Павлодар, 2024

Концепция воспитательной работы со школьниками как парадигмы кибербезопасности разработана в рамках грантового проекта Комитета науки Министерства науки и высшего образования Республики Казахстан АР19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента».

Разработчики:

Ж.О. Жилбаев – к.п.н., и.о. председателя правления – ректор НАО «Павлодарский педагогический университет им. Ә. Марғұлан», руководитель проекта

Д.Б. Абыкенова – доктор PhD, ассоциированный профессор высшей школы естествознания НАО «Павлодарский педагогический университет им. Ә. Марғұлан», главный научный сотрудник проекта

Ж.Н. Матенова – руководитель Комплаенс - службы - комплаенс-офицер НАО «Торайгыров университет», старший научный сотрудник проекта

А.Ж. Асаинова – к.п.н., профессор, директор Центра педагогических исследований НАО «Павлодарский педагогический университет им. Ә. Марғұлан», ведущий научный сотрудник

Л.С. Сырымбетова – д.п.н., профессор, заведующая кафедрой физической культуры и спортивного менеджмента Карагандинского университета Казпотребсоюза, главный научный сотрудник проекта

З.К. Кульшарипова – к.п.н., ассоциированный профессор (доцент) высшей школы педагогики НАО «Павлодарский педагогический университет им. Ә. Марғұлан», ведущий научный сотрудник

Рассмотрена на Учебно-методическом совете НАО «Павлодарский педагогический университет им. Ә. Марғұлан» протокол №4 от «16» февраля 2024 г.

Утверждена решением Ученого совета (протокол №6 от «28» февраля 2024 г.)

Содержание

1. Нормативные ссылки
2. Глоссарий
3. Введение
4. Анализ текущей ситуации
5. Цель и задачи Концепции
6. Подходы и принципы воспитательной работы в рамках обеспечения кибербезопасности школьной среды
7. Механизмы обеспечения информационной безопасности личности
8. Направления воспитательной работы по повышению у школьников навыков кибербезопасности
9. Мониторинг и оценка
10. Ожидаемые результаты реализации Концепции

1. Нормативные ссылки

В настоящей Концепции воспитательной работы со школьниками как парадигмы кибербезопасности (далее – Концепция) использованы следующие нормативные и правовые акты:

I Законодательство

1. Закон Республики Казахстан «Об образовании» от 27 июля 2007 года № 319-III (с изменениями на: 23.02.2024).

2. Закон Республики Казахстан от 24.11.2015 г. «Об информатизации».

3. Закон Республики Казахстан от 05.07.2004 г. «О связи».

II Постановления Правительства Республики Казахстан

4. 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».

5. Концепция кибербезопасности ("Киберщит Казахстана"). Утверждена Постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями на: 17.03.2023).

6. Концепция развития дошкольного, среднего, технического и профессионального образования Республики Казахстан на 2023-2029 годы. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 249.

7. Постановление Правительства Республики Казахстан от 20.12.2016 г. № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

8. Постановление Правительства Республики Казахстан от 09.08.2018 г. № 488 «Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности».

III Приказы государственных органов Республики Казахстан

9. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28.03.2018г. № 52/НК «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры».

10. Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 16.08.2019г. № 199/НК «Об утверждении Правил проведения мониторинга событий информационной безопасности объектов информатизации государственных органов».

11. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19.03.2018 г. № 48/НК. «Об утверждении Правил обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной

безопасности и Национальным координационным центром информационной безопасности».

12. Приказ Комитета национальной безопасности Республики Казахстан от 27.03.2018г. № 25/нс «Об утверждении Правил функционирования системы централизованного управления сетями телекоммуникаций Республики Казахстан».

13. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 28.10.2022 г. № 400/НК «Об утверждении правил формирования и ведения реестра статических адресов сетей передачи данных».

14. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 13 октября 2020 года № 386/НК «Об утверждении Правил функционирования единого шлюза доступа к Интернету и единого шлюза «электронной почты электронного правительства».

15. Приказ Комитета национальной безопасности Республики Казахстан от 27.03.2018г. № 24/нс «Об утверждении Правил присоединения сетей операторов междугородной и международной связи к точкам обмена интернет-трафиком и пропуска интернет-трафиком».

16. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 16.03.2018 г. № 44/НК «Об утверждении Правил создания и обеспечения функционирования единой национальной резервной платформы хранения электронных информационных ресурсов».

17. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 16.03.2018 г. № 45/НК «Об утверждении Правил передачи резервных копий электронных информационных ресурсов на единую платформу резервного хранения электронных информационных ресурсов».

18. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 03.06.2019 г. № 111/НК «Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности».

19. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29.06.2019 г. № 144/НК «Об утверждении Правил проведения экспертизы в сфере информатизации инвестиционных предложений, финансово-экономических обоснований бюджетных инвестиций».

20. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29.06.2019 г. № 143/НК «Об утверждении Правил составления и рассмотрения технических

заданий на создание и развитие объектов информатизации «электронного правительства».

21. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30.04.2021 г. № 156/НК «Об утверждении Правил осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах».

22. Приказ Председателя Комитета национальной безопасности Республики Казахстан от 27.10.2020 г. № 69-ке «Об утверждении Правил функционирования Национальной системы видеомониторинга».

2.Глоссарий

В настоящей Концепции применяются следующие понятия и их определения:

Воспитание — это целенаправленное и планомерное воздействие на умственное и физическое развитие детей, формирование их морального облика.

Интернет — это глобальная сеть, которая объединяет огромное количество компьютеров по всему земному шару и дает возможность получения доступа к информационным ресурсам.

Информационная безопасность — состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Кибератака — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Кибербезопасность — состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

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.

Киберинцидент — событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности.

Киберугроза — это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей.

Компьютерный вирус - это вид вредоносного программного обеспечения, которое способно распространять свои копии с целью заражения и повреждения данных на устройстве жертвы. Вирусы могут попасть на компьютер из других уже зараженных устройств, через носители информации (CD, DVD и т.п.) или через Интернет-сеть.

Мониторинг — это непрерывный процесс наблюдения и регистрации параметров объекта, сравнения их с заданными стандартами.

Образовательная среда - совокупность условий, необходимых для обучения, воспитания и развития человека, становления его личности.

Персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Казахстан внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо.

Развитие - это совершенствование сформированных способностей в направлении достижения количественных и качественных показателей, установленных профессиональными стандартами, которые, в свою очередь, задаются потребностями соответствующих сфер жизнедеятельности общества и человека.

Фишинг – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.).

Цифровая грамотность — это набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых инструментов, технологий и интернета.

3. Введение

Актуализация проблемы воспитательной работы со школьниками как парадигмы кибербезопасности неизбежно вызывает достаточно традиционные вопросы, ответы на которые необходимо ставить с учетом специфики, профиля, реальных культурно-информационных возможностей, общей программы развития образования.

Основные функции Концепции воспитательной работы со школьниками как парадигмы кибербезопасности - обеспечить методологические, теоретические и методические основы качественной организации информационной безопасности и обучать детей киберграмотности, обозначить сущностные критерии и ориентиры обучающейся молодежи, конкретизировать целевую направленность, предложить идеи и вектор воспитания будущего специалиста с высшим образованием. Концепция воспитательной работы со школьниками как парадигмы кибербезопасности строится с учетом актуализации и модернизации, и высшего педагогического образования в Республике Казахстан, в сочетании с принципом преемственности всех уровней образования и сохранения, преумножения лучших воспитательных традиций, практик и опыта, накопленных в историю казахстанского образования.

Концепция воспитательной работы со школьниками как парадигмы кибербезопасности содержит общие положения и принципы организации воспитательной работы в условиях кибербезопасности, сложившиеся к настоящему времени, и учитывает возможные изменения социально-информационной среды казахстанского образования в целом. Это предполагает ее дальнейшее совершенствование и коррекцию.

В разработке Концепции исходными документами являлись:

I Законодательство

1. Закон Республики Казахстан от 24.11.2015 г. «Об информатизации».
2. Закон Республики Казахстан от 05.07.2004 г. «О связи».

II Постановления Правительства Республики Казахстан

3. 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».

4. Постановление Правительства Республики Казахстан от 20.12.2016 г. № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

5. Постановление Правительства Республики Казахстан от 09.08.2018 г. № 488 «Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности».

III Приказы государственных органов Республики Казахстан

6. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28.03.2018г. № 52/НК «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры».

7. Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 16.08.2019г. № 199/НК «Об утверждении Правил проведения мониторинга событий информационной безопасности объектов информатизации государственных органов».

8. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19.03.2018 г. № 48/НК. «Об утверждении Правил обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности».

9. Приказ Комитета национальной безопасности Республики Казахстан от 27.03.2018г. № 25/нс «Об утверждении Правил функционирования системы централизованного управления сетями телекоммуникаций Республики Казахстан».

10. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 28.10.2022 г. № 400/НК «Об утверждении правил формирования и ведения реестра статических адресов сетей передачи данных».

11. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 13 октября 2020 года № 386/НК «Об утверждении Правил функционирования единого шлюза доступа к Интернету и единого шлюза «электронной почты электронного правительства».

12. Приказ Комитета национальной безопасности Республики Казахстан от 27.03.2018г. № 24/нс «Об утверждении Правил присоединения сетей операторов междугородной и международной связи к точкам обмена интернет-трафиком и пропуска интернет-трафиком».

13. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 16.03.2018 г. № 44/НК «Об утверждении Правил создания и обеспечения функционирования единой национальной резервной платформы хранения электронных информационных ресурсов».

14. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 16.03.2018 г. № 45/НК «Об утверждении Правил передачи резервных копий электронных информационных ресурсов на единую платформу резервного хранения электронных информационных ресурсов».

15. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 03.06.2019 г. №

111/НҚ «Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности».

16. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29.06.2019 г. № 144/НҚ «Об утверждении Правил проведения экспертизы в сфере информатизации инвестиционных предложений, финансово-экономических обоснований бюджетных инвестиций».

17. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29.06.2019 г. № 143/НҚ «Об утверждении Правил составления и рассмотрения технических заданий на создание и развитие объектов информатизации «электронного правительства».

18. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30.04.2021 г. № 156/НҚ «Об утверждении Правил осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах».

19. Приказ Председателя Комитета национальной безопасности Республики Казахстан от 27.10.2020 г. № 69-ке «Об утверждении Правил функционирования Национальной системы видеомониторинга».

Фундаментализация образования в Казахстане должна рассматриваться как база общекультурной, социальной и научно-технической основы формируемой системы знаний, культуры, современного мировоззрения, а также таких необходимых качеств у гражданского населения, как универсальность гуманитарного и инженерного знания, широта научно-технической мысли, способность к самообразованию, профессиональной мобильности; развитие материально-технической базы и социокультурной сферы (достаточное количество учебной литературы, компьютерных классов, учебно-методических кабинетов, читальных залов, лабораторий, оснащенных современным оборудованием приборами и т.д.); поиск наиболее эффективных путей и средств воспитания обучающихся во всех сферах их жизнедеятельности; организация и проведение социологических исследований.

Концепция основана на оценке текущей ситуации в сфере цифровизации образования Республики Казахстан. Концепция представляет собой рамочный документ по организации воспитательной работы в школе в целях обеспечения кибербезопасности образовательной среды.

Концепция призвана обеспечить единство подходов к мониторингу обеспечения кибербезопасности образовательной среды школы, а также

выработку механизмов предупреждения и оперативного реагирования на инциденты кибербезопасности.

Концепция 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 информационно-коммуникационных технологий (далее – ИКТ).

4. Анализ текущей ситуации

Внедрение онлайн сетей и удаленного доступа вносит особые риски в систему безопасности школ, таких как кибератаки, удаленное отключение оборудования, сбой процесса работы, хищение важной документации.

Внешние воздействия на киберсети школ могут привести как к ошибке в работе оборудования, так и к глобальным проблемам в виде остановки работы на длительный срок.

С целью минимизации подобных рисков, отдельного управления сетями и повышения безопасности разработан Техническим комитетом IEC 65 «Автоматизация, измерение и управление производственными процессами» стандарт кибербезопасности международного уровня СТ РК IEC/PAS 62443–3 «Сети коммуникационные школы. Защищенность (кибербезопасность) сети и системы. Защищенность (кибербезопасность) учебного процесса измерения и управления».

Стандарт безопасности включает в себя, в первую очередь:

- анализ структуры школьного образования, поиск возможных угроз и уязвимых мест;
- перевод и развитие существующих систем в школах;
- достижение целей безопасности с существующими технологиями на образовательное;
- обеспечение надежности и доступности защищенных коммуникационных сервисов;
- применимость к системам любого размера и риска;
- совместимость требований защиты, нормативно-правового соответствия и функциональности автоматики с требованиями безопасности.

По национальному индексу кибербезопасности Казахстан занял 78 место из 176 стран мира. Индекс кибербезопасности составил 48,05%. По оценке экспертов, Казахстан на 100% защищает свои персональные данные, на 89% – данные образования и профессионального развития. Защиту цифровых сервисов и военные кибероперации – на уровне 0%. Сфере разработки политики кибербезопасности присвоили 57%.

В мире растет число хакерских атак. В 2023 году от взломов пострадали более 75% всех мировых компаний по данным аналитического портала Statista. Пять лет назад показатель был на уровне 50%.

В Казахстане большая часть кибератак пришлось на заражение компьютеров вредоносными вирусами. Годовой рост – сразу на 69,1%. Количество фишинговых атак, то есть направленных на кражу номеров банковских карт, выросло сразу в 14 раз. Число атак ботнетов возросло почти в 2,5 раза. В то же время количество DDoS-атак, блокирующих работу сайта, уменьшилось на 20%. Убытки подсчитали и в лаборатории Касперского. Здесь также отметили рост фишинговых атак и шпионских программ. Как отмечают специалисты, несмотря на снижение, программы-вымогатели становятся более развитыми. Хакерские группировки, сумевшие взломать систему, шифруют данные.

В сфере детской/школьной кибербезопасности согласно результатам опроса, который был проведён агентством OnIn по заказу «Лаборатории Касперского» в декабре 2022 года и январе 2023 года, 38% родителей пользуются сервисами, к которым есть доступ и у детей. 11% респондентов подтвердили совместный доступ к онлайн-магазинам, 10% — к онлайн-кинотеатрам и стриминговым ресурсам, 9% — к облачным сервисам. Больше половины опрошенных отметили, что рассказывают своему ребёнку об онлайн-угрозах, 29% установили программу родительского контроля, 25% проверяют историю браузера. В основном родители контролируют детей с 4 до 11 лет. Они стремятся следить за тем, сколько времени те проводят в интернете, какими сайтами или программами пользуются. В результате ошибок детей в сети лишился денег примерно каждый десятый (9%) респондент. 47% потеряли от 4000 до 16000 тенге, 27% — до 4000 тенге, но были и те, кто потерял больше 400 тысяч тенге (1%). Дети могут случайно или намеренно оплатить какую-либо подписку, доступ к приложению или совершить покупку в игре. 58% родителей в Казахстане выкладывают в социальные сети посты или фото, а также видео со своими детьми, а больше половины (54%) респондентов делают это без согласия ребёнка. Чаще всего взрослые делятся в сети историями из жизни детей (48%), рассказывают об их увлечениях (36%). При этом почти треть (28%) раскрывает имя ребёнка.

Больше половины опрошенных (52%) знают о существовании хотя бы одной страницы своего ребёнка в социальных сетях. У 70% детей есть аккаунт в TikTok, у 62% — в YouTube, а у 27% — во ВКонтакте. По словам родителей, сами дети в открытом доступе размещают личные фотографии (59%), делятся данными об увлечениях и хобби (52%), возрасте (36%), реже сообщают такие подробности, как номер школы, номер мобильного телефона либо размещают фотографии с обстановкой квартиры. Некоторые респонденты ответили, что имеют доступ к одному из аккаунтов ребёнка: 28% опрошенных знают пароль на тот случай, если посчитают нужным зайти и проверить активность ребёнка в соцсетях, а 24% — не только знают пароль, но и пользуются им¹.

¹ Источник: <https://tribune.kz/kiberbezopasnost-naskolko-kazahstanskije-deti-zashhishheny/>

Преобразование обществ в информационно-ориентированные культуры требует смены парадигмы в системах образования. Школьные программы должны развиваться, чтобы вооружить учащихся необходимыми знаниями и навыками для безопасного и ответственного перемещения в сложном цифровом мире. Кибербезопасность, которую часто воспринимают как загадочную дисциплину, основанную на сложных алгоритмах и кодах, должна быть внедрена в основную систему образования. Школы должны преподавать кибербезопасность не только как часть компьютерного или технологического образования, но и как новую форму цифровой грамотности. Такое обучение вооружит молодежь способностью защищать свои данные и конфиденциальность, что становится все более ценным товаром в цифровом мире. Более того, это также поможет воспитать новое поколение профессионалов в области кибербезопасности, готовых охранять наши цифровые границы.

Ключевые проблемы рассматриваемого вопроса следующие:

- Отсутствие задач и направлений в Концепции кибербезопасности ("Киберщит Казахстана") и Концепции развития дошкольного, среднего, технического и профессионального образования Республики Казахстан на 2023–2029 годы, связанных с обеспечением кибербезопасности образовательной среды школы.

- Отсутствие на национальном уровне полной статистики по развитию цифровой грамотности и навыков кибербезопасности школьников.

- Отдельные исследования в данной области свидетельствуют об активности школьников в цифровой среде, о недостаточности уровня сформированности навыков кибербезопасности школьников и школьной среды.

5. Цели и задачи концепции воспитательной работы со школьниками как парадигмы кибербезопасности

Главная цель «Концепции воспитательной работы со школьниками как парадигмы кибербезопасности» 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.

Содержание Концепции раскрывает развитие антикризисных компетенций как способа борьбы с тем или иным видом киберугроз: «Проблемы интернет-зависимости», «Мошеннические действия в Интернете. Киберпреступления», «Правовые аспекты защиты киберпространства» и др.

Анализ этих разработок Концепции, а также изученных разработок, предлагаемых самими учителями, свидетельствует о том, что ведущим средством формирования навыков безопасного поведения в киберпространстве остаются материалы инструктивного характера или стандартов.

Понимая недостаточность данных материалов нами, предлагается дополнить их *ситуационными задачами на распознавание киберугроз и принятие правильных решений при встрече с ними.*

Разработка приоритетных задач для школы в рамках концепции обеспечения информационной безопасности детей включает несколько ключевых направлений. Вот основные задачи:

1. Внедрение образовательных программ по кибербезопасности
Интеграция кибербезопасности в учебный и внеучебный процесс:
 - Включение тем по кибербезопасности в школьный предмет Информатика.
 - Разработка и использование специализированных учебных материалов и пособий.
 - Проведение внеурочных занятий:
 - Организация семинаров и родительских собраний, посвященных кибербезопасности.
2. Создание безопасной цифровой среды в школе
 - Установка и регулярное обновление антивирусного программного обеспечения и систем фильтрации контента на школьных компьютерах.
 - Настройка и поддержка безопасных сетевых соединений.
 - Разработка и внедрение политик по использованию интернет-ресурсов в школе.
 - Организация системы мониторинга активности учащихся в интернете.
3. Подготовка педагогов и сотрудников
 - Проведение тренингов и курсов для педагогов по вопросам кибербезопасности.
 - Разработка методических рекомендаций для учителей по обучению кибербезопасности.
 - Регулярное информирование педагогического коллектива о новых угрозах и способах их предотвращения.
 - Организация обмена опытом и лучшими практиками среди сотрудников школы.
4. Воспитательная работа с учащимися
 - Обучение безопасному поведению в интернете:
 - Проведение классных часов и бесед на тему кибербезопасности.
 - Использование интерактивных методов обучения (игры, викторины, проекты).
 - Обучение учащихся анализу и оценке информации из интернета.
 - Формирование навыков противодействия дезинформации и фейковым новостям.
5. Взаимодействие с родителями
 - Проведение родительских собраний и консультаций на тему кибербезопасности.

- Распространение информационных материалов (буклетов, памяток и т.д.) по вопросам защиты детей в интернете.
- Организация совместных мероприятий с участием родителей и учащихся (семинары, мастер-классы).
- Создание родительских комитетов или групп по вопросам кибербезопасности.

6. Профилактика и реагирование на инциденты

- Разработка и внедрение программ по профилактике кибербуллинга и других киберугроз.
- Проведение регулярных опросов и анкетирований для выявления проблем и угроз.
- Создание системы поддержки и помощи для учащихся, столкнувшихся с киберугрозами.
- Разработка четких инструкций и алгоритмов действий при возникновении инцидентов кибербезопасности.

7. Сотрудничество с внешними организациями

- Привлечение экспертов для проведения обучающих мероприятий и консультаций.
- Участие в совместных проектах и инициативах по кибербезопасности.
- Участие в государственных и общественных программах по кибербезопасности.
- Обмен информацией и лучшими практиками с другими образовательными учреждениями.

Эти задачи направлены на создание комплексной системы обеспечения информационной безопасности в школе, способствующей формированию у учащихся навыков безопасного и ответственного поведения в цифровом пространстве.

Именно такие задачи и предлагались участникам проекта, проведенного в Павлодарской и Кызылординской области в рамках проекта «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс менеджмента» в октябре 2023-2024 года.

В школах детям при встрече были розданы «Памятка для обучающихся об информационной безопасности»:

НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);

2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;

3. Грубить, придирается, оказывать давление - вести себя невежливо и агрессивно;

4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;

5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;

2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;

3. Незаконное копирование файлов в Интернете - воровство;

4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;

5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО

1. Уважай других пользователей;

2. Пользуешься Интернет-источником - делай ссылку на него;

3. Открывай только те ссылки, в которых уверен;

4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут;

5. Пройди обучение на сайте нашего проекта и получи паспорт цифрового гражданина.

Кроме практических рекомендаций к результатам разработки концепции их представлены примеры учебных занятий, отнесенных к разным предметам и ориентированных на решение задач обучения учащихся кибербезопасности.

Настоящая Концепция определяет цели, задачи, принципы и основные направления развития воспитательной работы со школьниками как парадигмы кибербезопасности осуществляемой как в процессе учебы, так и во внеучебное время.

Модернизация и инновационное развитие - единственный путь, который позволит Республике Казахстан стать конкурентным обществом в мире 21-го века, обеспечить достойную жизнь всем нашим гражданам. В условиях решения этих стратегических задач в сфере информационных технологий «Урок цифры», знание квантовых технологий, криптографии, сенсорных симуляторов и как с их помощью учебные и воспитательные сферы в школе становятся безопаснее и технологичнее.

Цель Концепции: обеспечение воспитательной работы, направленной на достижение и поддержание уровня кибербезопасности школьников.

Задачи Концепции:

1. Создание необходимых условий для повышения осведомленности школьников о кибербезопасности.

2. Использование воспитательного потенциала учебных предметов для повышения цифровой грамотности школьников.

3. Обеспечение системного единства учебной и воспитательной работы в школе аспекте обеспечения кибербезопасности образовательной среды.

4. Определение механизмов диагностики цифровой грамотности школьников на основе постоянного мониторинга кибербезопасности образовательной среды.

6. Подходы и принципы воспитательной работы в рамках обеспечения кибербезопасности школьной среды

Парадигмальный подход, предполагающий наличие плана реагирования на киберинциденты, которые часто происходят неожиданно, четко прописанных процедур (какие действия, как и кем будут выполняться), которые повысят шансы на успех во время реальных киберинцидентов.

Междисциплинарный подход, который реализуется посредством соблюдения следующих принципов:

- принцип «воспитывать, обучая, и обучать, воспитывая», который реализует воспитательный потенциал учебных предметов;
- принцип целенаправленности педагогических воздействий для повышения грамотности школьников по вопросам кибербезопасности;
- принцип системности, который обуславливает логическую взаимоувязанность формирования у школьников навыков кибербезопасности и оценки их уровня;
- принцип комплексности, который обеспечивает единство воспитательной работы и работы с родителями школьников, а также работы по повышению квалификаций педагогов и руководителей школ.

В основу Концепции положены следующие подходы к организации воспитательной деятельности в условиях кибербезопасности:

– **аксиологический**: имеет целью введение формирующейся личности в мир ценностей и оказание ей помощи в выборе личностно значимой системы ценностных ориентаций. Благодаря ценностным ориентациям человек делает свою жизнь осмысленной, определяя ценности жизнедеятельности, переживаний, отношений;

– **системно - деятельный подход**: признание того, что личность проявляется и формируется в деятельности. Основная задача - формирование личности через деятельность;

– **личностно-ориентированный**: личность рассматривается как активный субъект собственного становления и развития; воспитательный процесс является антропоцентрическим по целям, содержанию и формам организации; задача педагога заключается в стимулировании, поддержке, активизации внутренних резервов развития личности;

– **комплексный подход**: позволяет учитывать следующую закономерность: факторы, влияющие на эффективность воспитательного процесса, тесно связаны между собой и возникают при определенных, специально создаваемых условиях, что дает возможность предвидеть характер и результаты функционирования воспитательного процесса, находить оптимальные пути и средства в его организации и проведении.

Использование данных подходов в выработке **«Концепция воспитательной работы со школьниками как парадигмы кибербезопасности»** позволяет включать вопросы психологии, педагогики, социологии профессионально-педагогической деятельности и реальной кадровой ситуации и информационной грамотности учителей, что является также одним из структурных компонентов воспитательной системы в целом.

На всех этапах введения **«Концепция воспитательной работы со школьниками как парадигмы кибербезопасности»** в школах будет реализовывать три основные специфические функции:

- защитная функция - создание благоприятных психологических условий включая кибербезопасность в учебно-воспитательном процессе школ, что является защитником законных интересов, интересов группы, гарантом соблюдения прав учащихся в образовательном процессе.

- диагностическая функция, - построение системы информационно – культурных отношений, безопасного общения в соцсетях, информационной деятельности, организацию самоуправления в школьной группе на основе анализа результатов психолого-педагогической диагностики личности отдельного обучающегося и состояния дел в школьной группе.

- посредническая функция - взаимодействие с родителями обучающихся с целью организации помощи в тех ситуациях, когда требуется участие семьи, выступает посредником в разрешении различных проблем обучающегося, ситуаций его жизнедеятельности с различными службами школы.

Интернет как мы знаем – это мир интересных и полезных возможностей в период обучения в школе, но в то же время это источник угроз. Стремительное развитие компьютерных технологий меняет школьное окружение и порождает множество новых проблем, в частности, проблему формирования информационной культуры, компьютерной грамотности, культуре поведения и безопасности в сети среди подрастающего поколения. Формирование личности обучающихся в условиях кибербезопасности личности школьника предполагает различные трактовки понятия «информационная безопасность», обосновывается необходимость применения витагенной технологии обучения с целью формирования информационно-личностной безопасности школьника.

Основными принципами организации системы обучения и воспитания в современных условиях кибербезопасности личности школьника должны стать:

- соответствие организации учебно-воспитательной работы и всей деятельности образовательных учреждений современным принципам развития (демократизации, гуманизации, активности личности и др.);

- единство научного, прикладного и практического аспектов функционирования системы воспитания;

- стремление к наиболее полному удовлетворению потребностей всех участников процесса обучения и воспитания; научное обеспечение развития системы обучения и воспитания обучающихся.

И тогда важнейшими качествами личности в Концепции воспитательной работы со школьниками как парадигмы кибербезопасности становятся инициативность, способность творчески мыслить и находить нестандартные решения, умение выбирать профессиональный путь, готовность обучаться в течение всей жизни.

7. Механизмы обеспечения информационной безопасности личности

За основу разработки содержания задач концепции взяты тематические материалы методических рекомендаций «Основы кибербезопасности». Они детализированы с учетом возрастных особенностей, интересов и деятельности учащихся в киберпространстве.

В мировой практике используются различные механизмы обеспечения информационной безопасности личности (как отдельное направление работы – информационная безопасность детей), которые обобщенно можно представить следующим образом:

- создание систем саморегулирования (кодексов профессионального поведения, внедрение стандартов, положений, политик по кибербезопасности);
- воспитание у обучающегося ответственного пользования информационными ресурсами, формирование ответственной позиции со стороны учителей и родителей, использование программно-технических средств и возможностей контентной фильтрации;
- контроль со стороны учебного заведения над содержанием информации в интернете, ограничение распространения среди обучающихся информации, пропагандирующей асоциальное поведение, связанной с проявлением ненависти, насилия;
- повышение осведомленности общественности, отдельных групп о проблеме информационной безопасности;
- мониторинг ситуации;
- проведение экспертизы информационной продукции, способной нанести вред здоровью и развитию человека; запретительные и ограничительные нормы в отношении рекламы некоторых групп товаров.

8. Направления воспитательной работы по повышению у школьников навыков кибербезопасности

Обучение и развитие навыков кибербезопасности у школьников

Примерная тематика воспитательных мероприятий по повышению у школьников навыков кибербезопасности

Примерная тематика и формы внеклассных мероприятий для учащихся 1-4 классов

1) Беседы и классные часы:
Что такое кибербезопасность?
Уход за устройством
Интернет-безопасность
Пароли

Личная информация.

2) Игры (конкурсы, викторины):

Я в безопасной интернет-среде

Лучшие пароли

Примерная тематика и формы внеклассных мероприятий для учащихся

5-9 классов

Тренинги «Общее цифровое гражданство»

Киберучения (индивидуальные в онлайн-режиме, классные, общешкольные)

Неделя кибербезопасности (в классе, в школе)

Конкурсы, викторины, игры:

Компьютерные вирусы

Методы защиты от вредоносных программ:

Сети WI-FI

Социальные сети

Электронные деньги

Электронная почта

Кибербуллинг или виртуальное издевательство

Мобильный телефон

Фишинг или кража личных данных

Примерная тематика и формы внеклассных мероприятий для учащихся

10-11 классов

Онлайн-курсы. Видеоигры. Онлайн-тренажеры. Классные часы:

Конфиденциальность в Интернете.

Безопасное общение

Безопасное использование устройств и соединений

Безопасность информации

Виртуальная и дополненная реальность

9. Мониторинг и оценка

Парадигмальный подход к организации воспитательной работы по кибербезопасности школьников предполагает разработку детального плана по реализации данной Концепции. Составление такого плана следует предварить комплексным психолого-педагогическим мониторингом кибербезопасных навыков и компетенций школьников. Лишь, исходя из анализа результатов первой (входной) диагностики, следует разработать план работы с учетом специфики и конкретных условий школы.

Структура мониторинга помимо отслеживания знаний, умений, навыков кибербезопасности школьников может включать состояние

цифровой инфраструктуры школы, компьютерной техники, интернет-сетей и др. к примеру:

1) Техносфера (техническая безопасность и базовая техническая грамотность пользователей). Сфера потребления (заказы, услуги, покупки, совершаемые онлайн). Информационная среда (создание, поиск, отбор, критическая оценка контента). Сфера коммуникации (создание, развитие, поддержание отношений, самопрезентация, идентичность, репутация).

2) Индекс цифровой грамотности: учащихся начальной школы, учащихся основной средней школы, учащихся старших классов, педагогов, руководителей школ, родителей школьников)

Важно, чтобы мониторинг проводился на постоянной основе, оценка кибербезопасности школьной среды должна проводиться регулярно, не реже одного раза в полгода.

10. Ожидаемые результаты реализации Концепции

Повышение уровня навыков кибербезопасности, школьников, педагогов, родителей.

Повышение уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Создание адаптивной системы управления кибербезопасностью школьной среды.