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
НАО «Павлодарский
педагогический университет
им. Ә.Марғұлан»
Председателя правления –
ректор Ж.О. Жилбаев

СТАНДАРТ

Обеспечения кибербезопасности образовательной среды школы

Павлодар

2024

Концепция воспитательной работы со школьниками как парадигмы кибербезопасности разработана в рамках грантового проекта Комитета науки Министерства науки и высшего образования Республики Казахстан AP19678646 «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.)

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий стандарт обеспечения кибербезопасности образовательной среды школы (далее Стандарт) представляет руководство по менеджменту информационной кибербезопасности (КБ) в организациях образования, поддерживая, в частности, международные и национальные требования к системе менеджмента информационной безопасности в соответствии с законодательством и стандартами РК в сфере информационной безопасности. Выбор подхода к менеджменту КБ осуществляется организацией и зависит от сферы деятельности.

Настоящий стандарт предназначен для руководителей, преподавательского состава, работников организации образования, родительской общественности и обучающихся, а также, при необходимости, для внешних сторон, имеющих отношение к этому виду деятельности. Стандарт устанавливает требования к обеспечению КБ в средних школах.

Стандарт как надежный механизм обеспечения кибербезопасности принесет пользу всей системе образования. В настоящем документе предлагается поэтапный подход с определением краткосрочных, среднесрочных и долгосрочных задач в деле систематической реализации стандарта обеспечения кибербезопасности образовательной среды школы как стратегии кибербезопасности.

2. ЦЕЛЬ И ЗАДАЧИ СТАНДАРТА

Целью Стандарта является защита интересов потребителей и образовательных учреждений по вопросам качества защиты – кибербезопасности, процессов и услуг в информационном пространстве. Кроме того, Стандарт решает следующие задачи:

- повышение уровня кибербезопасности жизни или здоровья субъектов образовательной системы, и содействия соблюдению требований технических регламентов в направлении;
- повышение уровня кибербезопасности объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера;
- обеспечение научно-технического прогресса;
- повышение конкурентоспособности продукции, работ и услуг;
- рациональное использование ресурсов;
- техническая и информационная совместимость;
- сопоставимость результатов исследований (испытаний) и измерений, технических и экономико-статистических данных;
- взаимозаменяемость продукции.

3. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий Стандарт отражает основные аспекты системы менеджмента информационной безопасности, прописанные в Национальном стандарте РК «СТ РК ISO/IEC 27001-2023 Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности». Данный стандарт может применяться при разработке Стандартов кибербезопасности как методов защиты киберсреды школы.

Настоящий Стандарт рекомендован для применения учреждениями среднего общего образования.

2.1. Стандарт представляет руководство по обеспечению кибербезопасности школьной среды.

Настоящий Стандарт поддерживает общие концепции, определенные 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, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска.

Кибербезопасность – это новая концепция в системе среднего общего образования. Однако поскольку угрозы для кибербезопасности приобретают все более распространенный характер, этот вопрос занимает одно из центральных мест при обсуждении и анализе рисков и уязвимости в школьном, родительском сообществах.

2.2 Знание концепций, моделей, процессов и терминологии, изложенных в Стандарте, важно для полного понимания настоящего стандарта.

2.3 Настоящий Стандарт применим для организаций образования всех типов, планирующих осуществлять обеспечение кибербезопасности и управление рисками, которые могут скомпрометировать информационную безопасность учебного процесса.

2.4 Настоящий Стандарт определяет политику кибербезопасности в организациях образования, как систему документированных управленческих решений, направленных на защиту определенных защищаемых процессов и активов Школы.

2.5 Настоящий Стандарт является документом, доступным каждому работнику и обучающемуся Школы и представляет собой официально принятую руководством Школы систему взглядов на проблему обеспечения кибербезопасности, и устанавливает принципы построения системы управления информационной безопасностью (далее – СУИБ) на основе систематизированного изложения целей, процессов и процедур кибербезопасности Школы.

2.6 Настоящий Стандарт может быть предоставлен официальным представителям любых органов и ведомств Республики Казахстан, партнерам Школы, подрядным организациям и частным лицам, выполняющим работы для Школы, а также другим заинтересованным организациям и лицам как на территории Республики Казахстан, так и за ее пределами. Настоящий документ разработан с учетом накопленного опыта в сфере обеспечения безопасности информационных технологий рабочей группой и работниками Школы.

2.7 Настоящий Стандарт разработан с целью установления единого подхода в Школе к обеспечению информационной безопасности детей, что прогнозирует необходимость формирования у них представления об интернет-культуре и привитие грамотного использования сети интернет не только в образовательных, но и в развлекательных целях. Необходимо исключить доступ к сомнительным сайтам, развивать у учащихся способности к самостоятельному распознаванию недостоверной информации, защите самих себя от сетевого негатива, формировать у учащихся внутренние принципы безопасного поведения в интернет-среде.

2.8 С целью реализации настоящего Стандарта термин кибербезопасность включает в себя в том числе понятие информационной безопасности и безопасности информационных технологий в Школе.

2.9 Настоящий документ рекомендован для применения во всех подразделениях и всеми должностными лицами в Школе, обучающимися и родительской общественностью при обеспечении и управлении кибербезопасностью Школы.

2.10 Действие настоящего документа распространяется на деятельность всех подразделений Школы.

2.11 Требования настоящего документа распространяются на процессы предоставления сервисов в области информационных технологий, включая облачные сервисы, сервисы эксплуатации, технической поддержки, мониторинга и обслуживания сетевой инфраструктуры, вычислительных систем, комплексов и программного обеспечения, предоставляемых пользователям.

2.12 Согласно данному документу «информационная безопасность детей» - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

4. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем Стандарте использованы нормативные ссылки на следующие акты законодательства:

3.1. 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. При разработке настоящего Стандарта использованы следующие нормативные документы:

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/НҚ «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/НҚ «Об утверждении Правил проведения мониторинга событий информационной безопасности объектов информатизации государственных органов»

8. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от19.03.2018 г. № 48/НҚ. «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/НҚ «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/НҚ «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/НҚ «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/НҚ «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-қе «Об утверждении Правил функционирования Национальной системы видеомониторинга»

IV Стандарты

1. СТ РК 1.15-2019 «Технические комитеты по стандартизации. Порядок создания и деятельности».

2.СТ РК 34.015-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

3.СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования».

4.СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасности».

5. СТ РК ИСО/МЭК 13335-5-2008 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 5. Руководство по управлению защитой сети».

6. СТ РК ISO/IEC 15408-1-2017 «Информационные технологии. Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

7. СТ РК ISO/IEC 15408-2-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

8. СТ РК ISO/IEC 15408-3-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты».

5. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В стандарте применяются следующие термины и определения:

Анализ — это процедура мысленного или материального разделения целостного объекта (предмета, явления, процесса) на составляющие части (признаки, свойства, отношения) с целью их изучения.

Декларация приверженности – это уведомление всех участников образовательной среды об ответственности за реализацию процессов и соблюдении требований кибербезопасности в целях ее обеспечения.

Документ - зафиксированная на материальном носителе информация с реквизитами, позволяющими его идентифицировать;

Информация - сведения о предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;

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

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

Компетенции — это знания, умения, навыки, модели поведения и личностные характеристики, при помощи которых достигаются желаемые результаты.

Конфиденциальность (англ. confidence - доверие) — необходимость предотвращения утечки (разглашения) какой-либо информации.

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

Программное обеспечение – это совокупность программ на компьютере или другом устройстве.

Пользователь - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

Риск — возможность возникновения события, которое может повлиять на достижение поставленных целей.

Субъект - активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа;

Управление рисками — процесс принятия и выполнения управленческих решений, направленных на снижение вероятности возникновения неблагоприятного результата и минимизацию возможных потерь проекта, вызванных его реализацией.

6. СПЕЦИАЛИЗИРОВАННЫЕ КОМПЕТЕНЦИИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Базовые профессиональные компетенции (далее – БПК) – компетенции, формируемые в соответствии с требованиями к сотрудникам школ (администрация школы, учителя и персонал), которые они обязаны освоить в рамках настоящего Стандарта для решения общих задач в профессиональной деятельности.

Компетенции сформированы в соответствии с требованиями к субъектам образовательной деятельности и отражающие их способность решать специализированные задачи КБ в профессиональной деятельности.

Поиск уязвимостей для сотрудника школы (заведующего по информатизации, заведующего по учебной работе, администратора компьютерной техники):

Сотрудник школы должен знать и понимать:

– Различные методологии поиска уязвимостей информационных ресурсов школы, компьютерных сетей и приложений.

– Популярные методы атак со стороны злоумышленников.

– Найденные и опубликованные критические уязвимости в операционных системах и серверах.

– Особенности использования различных сканеров безопасности.

– Методологию составления отчета о проведенном поиске уязвимостей.

– Основные способы защиты от атак на типовые уязвимости приложений.

Анализ защищенности для сотрудника школы (заведующего по информатизации, заведующего по учебной работе, администратора компьютерной техники):

Сотрудник должен знать и понимать

– Способы и рекомендации по обследованию объектов защиты и обобщения данных о их состоянии.

– Отраслевые и межотраслевые индустриальные стандарты, а также иные внутренние и международные нормативные документы в области информационной безопасности.

– Общепринятые классификации угроз информационной безопасности.

– Типовые причины атак на информационные ресурсы и системы, их последствия.

– Основные способы защиты информационных систем, в том числе и веб-приложений, обеспечения безопасности и целостности данных от атак злоумышленников.

– Состав и актуальность последних обновлений операционных систем и программного обеспечения для обеспечения информационной безопасности.

Специалист должен уметь:

– Анализировать существующие методы и средства обеспечения информационной безопасности и предлагать меры по их совершенствованию и развитию.

– Собирать информацию по ИТ-инфраструктуре объекта защиты с целью выработки и принятия решений и мер по защите информации.

– Применять анализаторы защищенности веб-приложения, включая онлайн-сервисы оценки защищенности.

– Контролировать состояние объекта защиты, в том числе и в части соблюдения общепринятых или задокументированных в стандартах правил и норм.

– Оценивать риски информационной безопасности школы используя классификации веб-угроз.

– Разрабатывать модели угроз и нарушителя.

– Составлять отчеты и организационно-распорядительную документацию по результатам обследования.

– Разрабатывать рекомендации по повышению уровня защищенности.

К информации, запрещенной для распространения среди детей, относится:

– информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью;

– способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх;

– обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

– отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

– оправдывающая противоправное поведение;

– содержащая нецензурную брань.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

– информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

– вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, несчастного случая, аварии или катастрофы и (или) их последствий;

– содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

7. ПРЕДПОСЫЛКИ СОЗДАНИЯ СТАНДАРТА

7.1 Систематический подход к обеспечению кибербезопасности и управлению рисками в сфере КБ необходим для того, чтобы идентифицировать потребности организации, касающиеся требований КБ, и создать эффективную систему обеспечения КБ. Этот подход дол жен соответствовать условиям деятельности организации и, в частности, должен быть согласован с общим менеджментом рисков в масштабе организации. Усилия по обеспечению кибербезопасности должны обеспечивать эффективное и своевременное реагирование на риски там и тогда, где и когда это необходимо. Управление рисками в сфере КБ должно быть неотъемлемой частью всех видов деятельности, связанных с обеспечением КБ, и должен применяться как на этапе внедрения, так и в процессе повседневного использования системы обеспечения КБ организации.

7.2 Обеспечение кибербезопасности и управление рисками в сфере КБ должны быть непрерывными процессами. В рамках данного процесса следует устанавливать контекст, оценивать и обрабатывать риски, используя для реализации рекомендации и решения плана обработки рисков. До принятия

решения о том, что и когда должно быть сделано для снижения риска до приемлемого уровня, в рамках менеджмента риска анализируется, что может произойти и какими могут быть возможные последствия.

7.3 Обеспечение кибербезопасности и управление рисками в сфере КБ должны способствовать:

- идентификации рисков;
- оценке рисков, исходя из последствий их реализации для деятельности организации образования и вероятности их возникновения;
- осознанию и информированию о вероятности и последствиях рисков;
- установлению приоритетов в рамках обработки рисков;
- установлению приоритетов мероприятий по снижению имеющих место рисков;
- привлечению причастных сторон к принятию решений о менеджменте риска и поддержанию их информированности о состоянии менеджмента риска;
- эффективности проводимого мониторинга обработки рисков;
- проведению регулярного мониторинга и пересмотра процесса менеджмента риска;
- сбору информации для совершенствования менеджмента риска;
- подготовке работников по вопросам рисков и необходимых действий, предпринимаемых для их уменьшения.

7.4 Обеспечение кибербезопасности и управление рисками в сфере КБ должны быть применены ко всей организации образования, к любой отдельной части организации (например, подразделению, отделу, службе), к любой информационной системе, к имеющимся, планируемым или специфическим аспектам управления.

7. 5 Общие правила для родителей

Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него.

Ваше внимание к ребенку - главный метод защиты.

Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты, на которых может упоминаться номер сотового телефона Вашего ребенка или Ваш домашний адрес.

Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за

опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

8. СВЕДЕНИЯ О СТАНДАРТЕ

Стандарт обеспечивает получение квалификации «Специалист по кибербезопасности».

8.1 Направление квалификации предусматривает следующие формы получения подтверждение квалификации и прохождение программы с получением сертификата на 72 ч.

8.2 Основными видами профессиональной деятельности специалиста может осуществляется иными видами профессиональной деятельности при условии соответствия уровня его образования и приобретенных компетенций требованиям к квалификации работника.

8.3 ПОДГОТОВЛЕН Рабочей группой научного проекта AP19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента»

9. ДЕКЛАРАЦИЯ ПРИВЕРЖЕННОСТИ АДМИНИСТРАЦИИ И РАБОТНИКОВ ШКОЛЫ

9.1. Администрация и педагогический состав Школы осознают важность и необходимость развития и совершенствования мер и средств обеспечения кибербезопасности в контексте развития законодательства и норм регулирования деятельности по защите информации, а также развития защищенных облачных технологий. Соблюдение требований кибербезопасности позволит создать конкурентные преимущества Школы, обеспечить её стабильность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

9.2. На администрацию Школы возлагается ответственность за организацию деятельности по обеспечению кибербезопасности, процесса анализа и оценки пригодности системы защиты информации, ее адекватности, результативности и возможностям улучшения.

9.3. Ответственность за реализацию процессов по обеспечению кибербезопасности в Школе возлагается на администрацию, педагогический состав и каждого работника Школы.

9.4. Администрация Школы должно обеспечить мотивацию персонала по обеспечению кибербезопасности Школы.

10. ЦЕЛИ И ЗАДАЧИ

10.1. Целью обеспечения кибербезопасности является поддержание устойчивого функционирования Школы, защита процессов с целью

установления единого подхода в учреждениях образования к управлению безопасностью информации. Настоящий план – это "живой документ", который будет меняться по мере развития ситуации в области кибербезопасности и будет регулярно обновляться с целью отразить требуемые изменения, вытекающие, помимо прочего, из анализа пробелов и мероприятий, изложенных в документе.

10.2. Общими целями Школы являются:

- развитие информационных и облачных технологий в Республике Казахстан;
- расширение количества и улучшение качества оказываемых образовательных услуг;
- развитие отношений с партнерами;
- повышение качества управления Школой посредством.

10.3. Целями обеспечения кибербезопасности в Школе являются:

- устойчивое функционирование и развитие Школы, обеспечение непрерывности предоставления образовательных услуг;
- обеспечение постоянного, открытого, прозрачного управления и контроля процессов обеспечения кибербезопасности.

10.4. Защищенность активов Школы оценивается и обеспечивается по каждому из следующих аспектов:

- доступность;
- целостность;
- конфиденциальность.

10.5. При этом критерием оценки является вероятность, размер и последствия нанесения Школе любого вида ущерба (невыполнение обязательств, финансовые потери, потеря репутации и пр.).

10.6. Целями построения системы управления информационной безопасностью в Школе являются:

- снижение актуальных рисков кибербезопасности и одновременное выполнение требований законодательства и нормативно-правовых актов Республики Казахстан, применением типовых наборов средств защиты информации;
- обеспечение процесса расследования инцидентов, связанных с безопасностью информации, сбора доказательной базы для отстаивания интересов Школы;
- определение ответственности между подразделениями Школы за обеспечение кибербезопасности.

10.7. Задачами построения системы управления информационной безопасностью в Школе являются:

- защита конфиденциальной информации в соответствии с законодательством Республики Казахстан, а также информации, определенной Школой, как нуждающейся в ограничении распространения;
- обеспечение выполнения требований нормативно-правовых документов в сфере информационной безопасности Республики Казахстан;

- организация управления рисками, связанными с нарушением безопасности информационных активов Школы, при котором риски постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска, либо имеется четкий план со сроками по их снижению/передаче;
- обеспечение непрерывности деятельности Школы на основе комплекса организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты информационных активов, а также направленных на бесперебойное оказание образовательных услуг;
- управление инцидентами, связанными с безопасностью информации, при этом любой факт (инцидент) нарушения требований по информационной безопасности рассматривается как существенное событие и требует разбирательства;
- минимизация потерь и скорейшее восстановление инфраструктуры, программных и технических средств, а также информации, вследствие кризисных (нештатных) ситуаций. Расследование причин возникновения таких ситуаций и принятие мер по их предотвращению в будущем;
- внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе системы управления информационной безопасностью;
- наращивание компетенции администрации, педагогического состава и работников Школы, обучающихся и родительской общественности в области кибербезопасности, что позволяет повышать качество услуг, оказываемых Школой.

11. ПРИНЦИПЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ

11.1. Школа в области кибербезопасности руководствуется следующими основными принципами:

Законность защиты: защита активов Школы соответствует положениям и требованиям действующих законов и иных нормативных правовых актов Республики Казахстан.

Системность защиты: системный подход к обеспечению кибербезопасности означает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения задачи обеспечения кибербезопасности в Школе.

Комплексность защиты: кибербезопасность обеспечивается эффективным сочетанием организационных, методических мер и программно-технических средств. Применение различных средств и технологий защиты процессов и активов снижает вероятность реализации наиболее значимых угроз кибербезопасности.

Непрерывность защиты: означает, что процессы кибербезопасности функционируют на всех этапах работы с активами Школы. В Школе осуществляется постоянный мониторинг и аудит процессов кибербезопасности.

Своевременность: означает упреждающий характер принимаемых мер по обеспечению кибербезопасности.

Гибкость: предполагает, что в процессе эксплуатации активов Школы изменения характеристик, объёма и категорий обрабатываемой информации влекут за собой своевременные и адекватные изменения в структуре управления кибербезопасностью.

Непрерывность совершенствования: означает, что меры и средства защиты активов постоянно совершенствуются в соответствии с результатами анализа функционирования структуры кибербезопасности, учитывается появление новых способов и средств реализации угроз кибербезопасности, а также принимается во внимание имеющийся отечественный и зарубежный положительный опыт в сфере кибербезопасности. В процессе непрерывного совершенствования осведомленности работников в части кибербезопасности проводится периодическое обучение.

Документированность: документирование обеспечивает закрепление достигнутого текущего состояния обеспечения кибербезопасности. Любые изменения этого состояния оформляются документально.

Разумная достаточность и адекватность: принимаемые меры обеспечения кибербезопасности эффективны и соразмерны имеющим место рискам кибербезопасности, связанных с обработкой и характером защищаемых активов, на основании результатов оценки рисков кибербезопасности; программно-технические средства и организационные меры, направленные на защиту активов, проектируются и внедряются таким образом, чтобы не повлечь за собой существенное ухудшение основных функциональных характеристик, а также производительности информационных систем и работников Школы.

Осведомленность о риске кибербезопасности: процессы обеспечения кибербезопасности затрагивают каждого работника, обучающегося Школы, использующего ее информационные активы, и накладывают на него соответствующие обязанности и ограничения.

Персональная ответственность: означает, что ответственность за обеспечение безопасности активов возлагается на каждого работника в пределах его полномочий.

Минимизация полномочий: любому работнику Школы доступ к информационным активам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий ограничены, контролируются и осуществляются строго в соответствии с установленными процедурами.

Взаимодействие и сотрудничество: означает, что в коллективе Школы создана благоприятная атмосфера, способствующая осознанной

необходимости соблюдения установленных правил и оказания содействия в деятельности подразделений, обеспечивающих кибербезопасность.

Специализация и профессионализм: означает, что к разработке средств и реализации мер защиты активов привлекаются компетентные работники, наиболее подготовленные к конкретному виду деятельности по обеспечению кибербезопасности, имеющие опыт практической работы;

Кадровая политика (подбор персонала, мотивация работников), используемая в Школе, обеспечивает исключение или минимизацию возможностей работников Школы по нарушению системы информационной безопасности.

Обязательность контроля: неотъемлемой частью работ по обеспечению кибербезопасности является оценка эффективности системы защиты. С целью своевременного выявления и пресечения попыток нарушения, установленных правил обеспечения безопасности активов, в Школе определены процедуры постоянного контроля использования систем обработки и защиты информации, а результаты контроля подвергаются регулярному анализу.

Контроль со стороны руководства: руководство Школы на регулярной основе (не реже одного раза в год) рассматривает отчеты о состоянии кибербезопасности в Школе и фактах нарушений установленных требований, а также общие и частные вопросы кибербезопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы. Политика кибербезопасности и предложения по ее актуализации рассматриваются Руководством.

11.2. Принципы контроля состояния систем обеспечения кибербезопасности:

Для обеспечения высокого уровня контроля в отношении системы управления кибербезопасностью в Школе на постоянной основе проводится комплексный анализ существующих защитных механизмов и возникающих инцидентов кибербезопасности, а также периодически полный аудит всей системы защиты информации;

Процесс мониторинга состояния кибербезопасности включает в себя контроль качества функционирования организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов;

По результатам аудита уполномоченные работники и ответственные подразделения Школы в разумные сроки определяют действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

12. ПОРЯДОК ПРИНЯТИЯ, УТВЕРЖДЕНИЯ И ИЗМЕНЕНИЯ СТАНДАРТА

12.1. Внесение изменений в действующий документ организует руководитель Школы при наступлении одного из следующих условий:

- при необходимости по результатам анализа рисков, аудитов и проверок соответствия требованиям кибербезопасности;
- при получении сообщения о необходимости внесения изменений в документ от любого участника процесса, обнаружившего несоответствие в нем;
- при проведении организационных и структурных изменений в Школе, затрагивающих процессы управления кибербезопасностью;
- в связи с внесением изменений в законодательство;
- в связи с внесением изменений во внутренние документы Школы.

12.2. В целях поддержания актуальности и эффективности действий по обеспечению кибербезопасности данный документ должен пересматриваться не реже одного раза в год.

12.3. Ответственный за соблюдение периода пересмотра документа является руководитель Школы.

12.4. Внесение изменений в стандарт, его утверждение и порядок принятия осуществляется приказом директора Школы на основании решения Педагогического Совета.