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

УТВЕРЖДАЮ
Член правления - проректор
по научной работе
Б.С. Есенгельдин
«22» 11 2023 г.

ПОЛОЖЕНИЕ
о кибербезопасности школьной образовательной среды

Павлодар, 2023

РАЗРАБОТАНО:

Рабочей группой в рамках проекта AP19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента»:
Руководитель проекта - к.п.н, профессор Ж.О. Жилбаев
Главный научный сотрудник - PhD, ассоциированный профессор Д.Б. Абыкенова
Главный научный сотрудник - д.п.н., профессоор Л.С. Сырымбетова
Ведущий научный сотрудник - к.п.н., профессоор А.Ж. Асаинова
Старший научный сотрудник - Ж.Н. Матенова

В Положении представлены основные требования и рекомендации по обеспечению кибербезопасности в средней общеобразовательной школе. Положение является практическим руководством по управлению IT-политикой для административного и педагогического составов Школы, работников Школы, обучающихся и родительской общественности.

Оглавление

1. Назначение и область применения
2. Нормативные ссылки
3. Декларация приверженности руководства Школы
4. Цели и задачи
5. Принципы управления кибербезопасностью
6. Порядок принятия, утверждения и изменения положения

1. Назначение и область применения

1.1. Положение о кибербезопасности (далее – «Положение») определяет политику кибербезопасности в средней общеобразовательной школе (далее – «Школа»), как систему документированных управленческих решений, направленных на защиту определенных защищаемых процессов и активов Школы.

1.2. Настоящее Положение 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.

1.3. Настоящее Положение Школы может быть предоставлено 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.

1.4. Настоящее Положение разработано с целью установления единого подхода в Школе к управлению безопасностью информации.

1.5. В целях настоящего Положения термин кибербезопасность включает в себя в том числе понятие информационной безопасности и безопасности информационных технологий в Школе.

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

1.7. Действие настоящего документа распространяется на деятельность всех подразделений Школы.

1.8. 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. Нормативные ссылки

2.1. При разработке настоящего Положения использованы следующие нормативные документы:

1) Закон Республики Казахстан «Об образовании», № 351-VI ЗРК от 06.2005 г., с изменениями и дополнениями;

2) Закон Республики Казахстан «Об авторском праве и смежных правах», № 6-I от 10 июня 1996 года, с изменениями и дополнениями;
3) Закон Республики Казахстан «Об информатизации», № 418-V ЗРК от 24 ноября 2015 года, с изменениями и дополнениями;
4) Типовые правила деятельности организаций среднего образования (начального, основного среднего и общего среднего), Приложение 2 к приказу Министра просвещения Республики Казахстан от 31 августа 2022 года № 385 с изменениями и дополнениями;
5) Приказ Министра образования и науки Республики Казахстан «Об определении минимальных требований к программно-аппаратному комплексу и прикладному программному обеспечению, используемых в организациях образования» № 79 от 2 марта 2020 года.

3. Декларация приверженности администрации и работников Школы

3.1. 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.
3.2. 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.
3.3. Ответственность за реализацию процессов по обеспечению кибербезопасности в Школе возлагается на администрацию, педагогический состав и каждого работника Школы.
3.4. Администрация Школы должно обеспечить мотивацию персонала по обеспечению кибербезопасности Школы.

4. Цели и задачи

4.1. Целью обеспечения кибербезопасности является поддержание устойчивого функционирования Школы, защита процессов и активов, принадлежащих Школе, пользователям его программного обеспечения.
4.2. 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.

4.3. Целями обеспечения кибербезопасности в Школе являются:

– устойчивое функционирование и развитие Школы, обеспечение непрерывности предоставления образовательных услуг;
– гарантия защищенности процессов и активов, принадлежащих Школе и пользователям его программного обеспечения;
– обеспечение постоянного, открытого, прозрачного управления и контроля процессов обеспечения кибербезопасности.
4.4. Защищенность активов Школы оценивается и обеспечивается по каждому из следующих аспектов:
– доступность;
– целостность;
– конфиденциальность.
4.5. При этом критерием оценки является вероятность, размер и последствия нанесения Школе любого вида ущерба (невыполнение обязательств, финансовые потери, потеря репутации и пр.).
4.6. 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.
4.7. Задачами построения системы управления информационной безопасностью в Школе являются:
– определение активов, подлежащих защите;
– 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.

5. Принципы управления кибербезопасностью

5.1. 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.

5.2. 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.

6. Порядок принятия, утверждения и изменения положения

6.1. 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 кибербезопасность;
- в связи с внесением изменений в законодательство;
- в связи с внесением изменений во внутренние документы Школы.

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

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

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