ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДЕТСКИЙ САД №93 КОМБИНИРОВАННОГО ВИДА
ВЫБОРГСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

«ПРИНЯТО»
на заседании Общего собрания
Протокол № 1 «09» 01.2023

«УТВЕРЖДЕНО»
Заведующим ГБДОУ детского сада №93
Выборгского района Санкт-Петербурга
Приказ от «09» 01 2023 № 17
_____ Л.А. Виноградова

«СОГЛАСОВАНО»
С Профкомом организации
Протокол «09» 01 2023

ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ ГБДОУ ДЕТСКИЙ САД № 93 КОМБИНИРОВАННОГО ВИДА ВЫБОРГСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

1. НАЗНАЧЕНИЕ

1.1. Настоящий документ (далее – Политика) определяет политику кибербезопасности в ГБДОУ детский сад № 93 (далее – ДОУ), как систему документированных управленческих решений, направленных на защиту определенных защищаемых процессов и активов ДОУ, партнеров.

1.2. Настоящая Политика является документом, доступным каждому работнику ДОУ и представляет собой официально принятую руководством ГБДОУ детский сад № 93 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 ДОУ.

1.3. Настоящая Политика ДОУ может быть предоставлена официальным представителям любых органов и ведомств Российской Федерации, представителям органов сертификационного аудита, партнерам ДОУ, подрядным организациям и частным лицам, выполняющим работы для ДОУ, а также другим заинтересованным организациям и лицам на территории Российской Федерации. Политика разработана на русском языке, в соответствии с законодательством Российской Федерации, а также с учетом накопленного опыта в сфере обеспечения безопасности информационных технологий в ДОУ.

1.4.Настоящая Политика разработана с целью установления единого подхода в ДОУ к управлению безопасностью информации.

1.5.В целях настоящей Политики термин «кибербезопасность» включает в себя в том числе понятие информационной безопасности и безопасности информационных технологий ДОУ.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Политика обязательна для применения во всех подразделениях и всеми работниками ДОУ, при обеспечении и управлении кибербезопасностью ДОУ.

2.2. Положения Политики распространяются на все аспекты деятельности ДОУ, тем или иным образом влияющие на кибербезопасность активов, партнеров и самой ДОУ.

2.3. Действие Политики распространяется на деятельность всех подразделений ДОУ.

2.4. 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 внешним и внутренним партнерам.

3. ДЕКЛАРАЦИЯ ПРИВЕРЖЕННОСТИ РУКОВОДСТВА ДОУ

3.1. Руководство ДОУ осознает 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, а также обеспечение конфиденциальности персональных данных позволит создать конкурентные преимущества ДОУ, обеспечить её стабильность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

3.2. Руководство ДОУ обязуется по согласованию с учредителем обеспечивать необходимыми ресурсами на поддержку и модернизацию СУИБ в соответствие с требованиями с Законодательством РФ.

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

3.4. Ответственность за реализацию процессов обеспечению кибербезопасности в ДОУ возлагается на Руководство ДОУ и каждого работника ДОУ.

3.5. Руководство ДОУ должно обеспечить мотивацию персонала по обеспечению кибербезопасности ДОУ.

4. ЦЕЛИ И ЗАДАЧИ

4.1. Общими целями ДОУ являются:

- развитие информационных и облачных технологий в ДОУ;
- расширение количества и улучшение качества оказываемых услуг за счет применения новых технологий, в том числе облачных сервисов, облачных вычислений и облачного хранения данных;
- расширение географии деятельности ДОУ;
- развитие отношений с российскими и зарубежными партнерами;

4.2. Целями обеспечения кибербезопасности в ДОУ являются:

- устойчивое функционирование и развитие ДОУ, обеспечение непрерывности предоставления услуг;
- гарантия защищенности процессов и активов, принадлежащих ДОУ;
- обеспечение постоянного, открытого, прозрачного управления и контроля процессов обеспечения кибербезопасности и защиты персональных данных.

4.3. Защищенность активов ДОУ оценивается и обеспечивается по каждому из следующих аспектов:

- доступность;
- целостность;
- конфиденциальность.

4.4. При этом критерием оценки является вероятность, размер и последствия нанесения ДОУ любого вида ущерба.

4.6. Задачами СУИБ ДОУ являются:

- определение активов, подлежащих защите;
- защита конфиденциальной информации в соответствии с законодательством Российской Федерации, в том числе, но не ограничиваясь: персональных данных, сведений, составляющих коммерческую тайну, информации, полученной при осуществлении деятельности ДОУ из других источников, а также информации, определенной Компанией, как нуждающейся в ограничении распространения;
- обеспечение выполнения требований нормативных правовых актов Российской Федерации в сфере информационной безопасности;
- организация управления рисками, связанными с нарушением безопасности информационных активов ДОУ, при котором риски постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска, либо имеется четкий план со сроками по их снижению;
- управление инцидентами, связанными с безопасностью информации, при этом любой факт (инцидент) нарушения требований по информационной безопасности рассматривается как существенное событие и требует разбирательства;
- противодействие новейшим комплексным угрозам кибербезопасности;
- 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;
- регулярная оценка соответствия СУИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов, мониторинга эффективности процессов СУИБ, анализа со стороны руководства ДОУ;
- внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СУИБ внутренним и внешним требованиям.

4.7. В результате реализации целей кибербезопасности и, в частности, целей и задач СУИБ в ДОУ разработан и внедрен комплекс организационно-методических и технических мероприятий.

4.8. Данные мероприятия являются базовой составляющей обеспечения и управления кибербезопасностью в ДОУ.

5. ПРИНЦИПЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ

5.1. Основные принципы управления кибербезопасностью.

ДОУ в области кибербезопасности руководствуется следующими основными принципами.

- Законность защиты:

защита активов ДОУ соответствует положениям и требованиям действующих законов и иных нормативных правовых актов Российской Федерации.

- 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 ДОУ.

- 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: функционирование процессов кибербезопасности на всех этапах работы с активами ДОУ. В ДОУ осуществляется постоянный мониторинг и аудит процессов кибербезопасности.
- Своевременность:

означает упреждающий характер принимаемых мер по обеспечению кибербезопасности.

- Гибкость:

предполагает, что в процессе эксплуатации активов ДОУ изменения характеристик, объёма и категорий обрабатываемой информации влекут за собой своевременные и адекватные изменения в структуре управления кибербезопасности.

- 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.

- Осведомленность о риске кибербезопасности:

процессы обеспечения кибербезопасности затрагивают каждого работника ДОУ, 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 трудовых обязанностей. Помимо этого, в ЦКЗ назначены ответственные лица за поддержание процессов обеспечения и управления кибербезопасности.

- Минимизация полномочий:

каждому работнику ДОУ доступ к информационным активам предоставляется только в том объеме, который необходим ему для выполнения трудовых 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 ДОУ создана благоприятная атмосфера, способствующая осознанной необходимости соблюдения установленных правил и оказания содействия в деятельности подразделений, обеспечивающих кибербезопасность.

- Разделение полномочий по управлению информационными технологиями:

в ДОУ реализована структура управления информационными технологиями, направленная на исключение конфликта интересов и строгое разграничение ответственности при обеспечении функционирования и безопасности информационных активов: разделены обязанности подразделений и работников ДОУ, осуществляющих администрирование коммуникационного оборудования, средств защиты, и осуществляющих функции мониторинга состояния кибербезопасности и контроля (аудита) выполнения требований кибербезопасности.

- Знание своих партнеров и работников:

ДОУ обладает информацией о своих партнерах, что позволяет минимизировать вероятность реализации угроз, связанных с человеческим фактором;

кадровая политика (подбор персонала, мотивация работников), используемая в ДОУ, обеспечивает исключение или минимизацию возможностей работников ДОУ по нарушению системы безопасности активов.

- 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 ДОУ определены процедуры постоянного контроля использования систем обработки и защиты активов, а результаты контроля подвергаются регулярному анализу.

- Контроль со стороны руководства:

руководство ДОУ на регулярной основе (не реже одного раза в год) рассматривает отчеты о состоянии кибербезопасности в ДОУ и фактах нарушений установленных требований, а также общие и частные вопросы кибербезопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнеспроцессы. Политика кибербезопасности и предложения по ее актуализации рассматриваются Руководством.

- Целевое финансирование мероприятий по обеспечению кибербезопасности:

ежегодный бюджет ДОУ предусматривает специальные статьи расходов на обеспечение кибербезопасности по согласованию с учредителем.

6. ВНЕСЕНИЕ ИЗМЕНЕНИЙ

6.1. Внесение изменений в Политику организует руководитель ДОУ при наступлении одного из следующих условий:

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

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

N версии документа	Содержание изменения	Ф.И.О. ответственного лица, внёсшего	Дата внесения изменения