СОГЛАСОВАНО
На Общем собрании работников
протокол № 3 от 15.03.2023 г.

УТВЕРЖДАЮ
И.о. заведующего
МБДОУ № 85 «Малиновка»
_____ Г.Л. Цыпко
приказ от 15.03.2023 г. № 258

ПОЛОЖЕНИЕ

Об ответственных за обеспечение информационной безопасности в МБДОУ № 85 «Малиновка»

I. Общие положения

1. Настоящее положение определяет цели, задачи и функции (далее – Положение) ответственных лиц муниципального бюджетного дошкольного образовательного учреждения «Детский сад № 85 «Малиновка» комбинированного вида» (далее – МБДОУ № 85 «Малиновка») в области в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, «Кодекс профессиональной этики МБДОУ № 85 «Малиновка» и настоящим типовым положением.

1.1. Настоящее Положение определяет полномочия, права и обязанности ответственных МБДОУ № 85 «Малиновка» за обеспечение информационной безопасности в органе (организации), в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее - ответственное лицо).
1.2. Ответственные лица определяется заведующим МБДОУ, и назначаются приказом.
1.3. Ответственные лица осуществляет свою деятельность на основе регламентов должностных инструкций работников МБДОУ № 85 «Малиновка».
1.4. Ответственные лица входят в состав коллегиальных органов МБДОУ № 85 «Малиновка».
1.5. Указания и поручения ответственных лиц в части обеспечения информационной безопасности являются обязательными для исполнения всеми работниками МБДОУ № 85 «Малиновка».

II. Квалификационные требования к ответственному лицу

2.1. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) и обязательно проходить раз в 3 года обучение по программе профессиональной подготовки по направлению "Информационная безопасность".
2.2. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:
а) основные процессы дошкольной образовательной организации и специфика обеспечения информационной безопасности организации;

а) основные процессы дошкольной образовательной организации и специфика обеспечения информационной безопасности организации;
б) влияние информационных технологий на деятельность организации, в том числе:
роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования организации;
зависимость основных процессов функционирования организации от информационных технологий;
в) информационно-телекоммуникационные технологии, в том числе:
современные информационно-телекоммуникационные технологии, используемые в организации;
г) способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее - системы и сети), в том числе ограниченного доступа;
типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;
принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей;
д) обеспечение информационной безопасности, в том числе:
цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;
цели обеспечения информационной безопасности применительно к основным процессам функционирования организации, реализации и контроля их достижения;
принципы и направления стратегического развития информационной безопасности в организации;
основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности организации для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности организации;
основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;
возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;
способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;
порядок организации взаимодействия внутри организации при решении вопросов обеспечения информационной безопасности;
планирование деятельности по обеспечению информационной безопасности в организации;
организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в организации;
обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;
организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы органа (организации) и реагированию на компьютерные инциденты;
организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в организации.

2.3. С учетом области и вида деятельности дошкольной организации от ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:
а) защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;
б) обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
в) создания и обеспечения безопасного функционирования информационных систем и информационных систем организации в защищенном исполнении;
г) создания, обеспечения технических условий установки и эксплуатации средств защиты информации; проверенной, безопасной и защищенной информации в которой отсутствует риск, связанный с причинением вреда здоровью и (или) развитию обучающихся; использование и классификацию информационной и учебно-методической продукции в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
д) иных нормативных правовых актов и стандартов в области информационной безопасности.

III. Трудовые (должностные) обязанности ответственного лица

3. Ответственные лица совместно с заведующим МБДОУ № 85 «Малиновка»:
а) организует разработку политики с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами организации, направленной в том числе на обеспечение и поддержание стабильной деятельности организации и ее процессов функционирования в случае проведения компьютерных атак; отвечает за согласование и утверждение политики в организации, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;
б) осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в организации, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в организации, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак;
осуществляет регулярное и своевременное информирование заведующего МБДОУ о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в организации и результатах практических учений по противодействию компьютерным атакам;
б) осуществляет контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым разделам работы;
в) осуществляет согласование требований к системам и сетям, оператором которых является организация в части обеспечения информационной безопасности;
организует работу по обеспечению информационной безопасности организации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену;
г) организует реализацию и контроль проведения в организации организационных и технических мер, решения о необходимости осуществления которых принимаются

Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю с учетом меняющихся угроз в информационной сфере, а также самостоятельно ответственным лицом в результате своей деятельности;
д) организует беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим организации, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет", в целях осуществления мониторинга их защищенности, а также работникам структурного подразделения, осуществляющего функции по обеспечению информационной безопасности;
е) контролирует исполнение педагогическими работниками соблюдения правовых, нравственных и этических норм при проведении образовательной работы с обучающимися или размещении информации для родителей (законных представителей) обучающихся в сети Интернет, в социальных группах ВКонтакте, Одноклассники, в Телеграм канале и других мессенджерах»; обеспечение защиты и конфиденциальности информации;
ж) организует формирование и развитие навыков работников организации в сфере информационной безопасности;
з) организует контроль пользователей информационных ресурсов организации в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;
и) организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в организации, осуществляет согласование иных документов организации в части обеспечения информационной безопасности;
к) обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".
л) повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

IV. Права ответственного лица

4. Ответственное лицо имеет право:
а) давать указания и поручения работникам организации в части обеспечения информационной безопасности;
б) запрашивать от работников организации информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей;
в) участвовать в заседаниях (совещаниях) коллегиальных органов организации, принятии решений по вопросам деятельности организации, а также по внесению предложений по совершенствованию деятельности организации;
г) участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу организации;
д) представлять результаты реализации политики коллегиальному органу организации;
е) принимать решения по вопросам обеспечения информационной безопасности организации;
ж) взаимодействовать с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и иными федеральными органами исполнительной власти по вопросам обеспечения информационной

безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности;
з) вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;
и) инициировать проверки уровня (состояния) обеспечения информационной безопасности в организации;
к) организовывать на объектах организации мероприятия по информационной безопасности, разработку и представление руководителю организации предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;
л) обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей ответственного лица.

V. Ответственность ответственного лица

5. Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность:
а) за неисполнение или ненадлежащее исполнение своих обязанностей;
б) за действия (бездействие), ведущие к нарушению прав и законных интересов организации;
в) за достижение целей обеспечения информационной безопасности;
г) за поддержание и непрерывное развитие информационной безопасности организации для исключения (невозможности реализации) негативных последствий;
е) за участие в организации мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности организации;
ж) за нарушения требований по обеспечению информационной безопасности;
з) за нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.
5.1. Педагогические работники подчинены по исполнению мероприятий по информационной безопасности заведующему МБДОУ или уполномоченному в организации, ответственному за обеспечение информационной безопасности в организации,
5.2. Контроль за деятельностью подразделения осуществляет заведующий МБДОУ № 85 «Малиновка»
5.3. Настоящее Положение действует и изменяется в соответствии действующими федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности.