Муниципальное автономное дошкольное образовательное учреждение Белоярского района «Детский сад «Звездочка» г. Белоярский»

УТВЕРЖДЕНО
Заведующий МАДОУ
«Детский сад «Звездочка» г. Белоярский»
_____ /Фокина С.С. /
Приказ № 189 от 31.08.2022 г.

Инструкция администратора безопасности в МАДОУ «Детский сад «Звездочка» г. Белоярский»

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Администратор безопасности в МАДОУ (далее – Администратор) назначается приказом заведующего МАДОУ и отвечает за информационную безопасность.

1.2. Администратор обязан поддерживать в актуальном состоянии свои знания законодательных, нормативно-правовых актов Российской Федерации и методических материалов в сфере информационной безопасности.

1.3. В своей деятельности Администратор руководствуется настоящей Инструкцией, Политикой информационной безопасности и действующим законодательством.

1.4. Администратор безопасности подчиняется напрямую Заведующему МАДОУ и имеет право требовать от пользователей выполнения указаний и инструкций, связанных с защитой информации.

1.5. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской

Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. ФУНКЦИИ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ.

2.1. Изучение особенностей и технологических процессов обработки информации в МАДОУ с целью принятия решения о необходимости защиты информации и классификации, либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации с сотрудниками сторонней организации. По окончании аналитических работ Администратор обязан ознакомиться с их результатами и подписать отчетные документы, либо составить мотивированный отказ в подписании таких документов и отправить их на доработку сторонней организации.

2.2. Определение актуальных угроз безопасности информации и разработка документа «Модель угроз безопасности», либо привлечение на договорной основе сторонних организаций для таких работ.

2.3. Периодический пересмотр актуальных угроз безопасности информации в следующих случаях:

- ежегодный плановый пересмотр актуальных угроз безопасности информации;
- появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки;
- существенное изменение условий функционирования, внедрение новых технологий;
- изменение нормативной документации, касающейся моделирования угроз безопасности информации;
- в результате инцидента безопасности.

2.4. Выработка предложений заведующему по совершенствованию системы защиты информации.

2.5. Ведение учета применяемых средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.

2.6. Обеспечение передачи конфиденциальной информации и персональных данных через сети связи общего пользования в зашифрованном виде.

2.7. Разработка плана мероприятий по обеспечению безопасности защищаемой информации и по защите периметра информационной системы. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.

2.8. Осуществление контроля физической сохранности и целостности технических средств, а также контроль сохранности и целостности опечатывающих пломб на технических средствах (в том числе и программно-аппаратных средствах защиты информации).

2.9. Организация учета съемных носителей информации. Настройка соответствующих программных механизмов средств защиты информации для запрета неучтенных съемных носителей. Ведение журнала учета съемных носителей.

2.10. Организация учета иных машинных носителей информации.

2.11. Проведение инструктажей сотрудников, работающих с защищаемой информацией, по темам: правила работы, защита информации, положения законодательства в сфере защиты информации, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников МАДОУ в вопросах информационной безопасности.

2.12. Организация первоначального доступа пользователям к ресурсам информационный системы в соответствии с утвержденным положением о разграничении прав доступа. Блокировка учетных записей, изменение полномочий пользователей и добавление новых пользователей в соответствии с Инструкцией о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам.

2.13. Осуществление резервного копирования.

2.14. Реализация горячего резервирования ключевых узлов (межсетевых экранов, серверов баз данных, сервера AD, криптошлюзов, коммутаторов, маршрутизаторов).

2.15. Организация резервных каналов связи и контроль обеспечения провайдером заявленных характеристик канала связи.

2.16. Осуществление контроля целостности программного обеспечения (в том числе и средств защиты информации). Периодически (не реже одного раза в месяц) сверять рассчитанные контрольные суммы ключевых системных и исполняемых файлов ПО и СЗИ с эталонными значениями.

2.17. Периодическое тестирование функций системы защиты, согласно плану мероприятий по обеспечению безопасности информации, либо при изменении программной среды.

2.18. Участие в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности. По мере возможности, Администратор должен восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а также восстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.

2.19. Контроль выполнения Пользователями требований Инструкции пользователя, а также других установленных требований для обеспечения безопасности.

2.20. В случае получения от Пользователей информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, Администратор незамедлительно принимает все необходимые меры для обеспечения безопасности, в пределах своих полномочий.

2.21. Обеспечение отсутствия на АРМ Пользователей средств разработки и отладки программного обеспечения. Контроль за отключением на АРМ Пользователей и невозможностью самостоятельного включения пользователем технологий мобильного кода (JavaScript, Adobe Flash, макросы MS Office и т. д.), кроме случаев, когда использование таких технологий необходимо для выполнения служебных (должностных) обязанностей.

2.22. Выявление уязвимостей посредством периодического сканирования системы сертифицированным сканером безопасности. Принятие решений на основании итогов каждого сканирования.

2.23. Контроль обновлений системного, прикладного программного обеспечения и средств защиты информации (в том числе обновлений антивирусных баз, сигнатур сценариев вторжений, информации об уязвимостях).

2.24. Контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств или настройку/установку программного обеспечения.

2.25. Обеспечение функционирования и поддержания работоспособности:
- системы защиты информации от несанкционированного доступа;
- системы межсетевого экранирования;
- системы обнаружения и предотвращения вторжений;
- системы криптографической защиты информации;
- системы антивирусной защиты.

2.26. Обеспечение непрерывности процессов. В случае нарушения работоспособности технических средств и программного обеспечения, в том числе средств защиты, Администратор принимает меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ.

Администратор имеет право:

3.1. Знакомиться с нормативными актами МАДОУ.

3.2. Вносить предложения заведующему по совершенствованию существующей системы защиты информации.

3.3. Требовать от Пользователей соблюдения требований Инструкции пользователя и иных нормативно-правовых и организационно-распорядительных документов по обеспечению информационной безопасности.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности.

3.5. Требовать прекращения работы, как в целом, так и отдельных Пользователей, в случае выявления нарушений требований по обеспечению безопасности.

3.6. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к Ответственному за организацию обработки персональных данных.

4. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦАНИРОВАННОГО ДОСТУПА.

4.1. Администратор участвует в развертывании средства защиты информации от несанкционированного доступа.

4.2. Администратор производит настройку подсистемы регистрации, идентификации и аутентификации. Идентификации и аутентификации подлежат как пользователи, так и учетные записи служб, приложений, программных процессов.

4.3. Удаленные (внешние) пользователи проходят идентификацию и аутентификацию. Администратор обеспечивает наличие минимального количества точек входа удаленных пользователей. Администратор производит мониторинг подключений и действий внешних пользователей. Администратор обеспечивает доступ внешних (удаленных) пользователей по защищенным каналам связи. Администратор предоставляет возможность удаленного доступа только тем пользователям, которым такой доступ необходим в силу исполнения ими служебных обязанностей.

4.4. Администратор осуществляет контроль использования мобильных технических средств (ноутбуки, нетбуки, планшеты, смартфоны и иные устройства). В случае использования мобильных устройств удаленными пользователями. Учет мобильных технических средств производится Администратором в Журнале учета портативных устройств, имеющих встроенные носители информации.

4.5. Администратор осуществляет учет машинных носителей информации, как стационарных (жесткие диски АРМ и серверов, SSD-накопители и т. д.), так и съемных (флеш-накопители, съемные жесткие диски, карты памяти, память мобильных устройств и т. д.). Каждому носителю присваивается идентификационный номер. Для стационарных машинных носителей информации фиксируется местонахождение носителя (АРМ, кабинет), в случае замены или утилизации стационарного, или съемного машинного носителя принимаются меры по гарантированному уничтожению информации на носителе или самого носителя с соответствующей пометкой в Журнале учета машинных носителей информации. Съемные машинные носители информации выдаются пользователям под роспись в Журнале учета приема/выдачи съемных машинных носителей информации. Дата сдачи машинного носителя также фиксируется в Журнале.

4.6. Администратор является ответственным за хранение, выдачу, инициализацию средств аутентификации (аппаратных ключей, учетных записей, первичных паролей). Администратор определяет парольную политику и требования к сложности паролей. Администратор выдает пользователю пароль для первоначального входа. Устанавливаются следующие требования к паролям:

- минимальная длина пароля составляет 8 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, как минимум одну цифру и один спецсимвол;
- при смене пароля, новый пароль должен отличаться минимум на два символа от предыдущего;
- максимальное время действия пароля – 90 дней;
- минимальное время действия пароля – 10 дней;
- запрещается использование пользователями пяти последних использованных паролей при создании новых паролей;

4.7. Администратор контролирует наличие и работоспособность средств доверенной загрузки.

4.8. Администратор запрещает пользователям самостоятельную установку любого программного обеспечения. Перечень разрешенного к установке программного обеспечения подлежит периодическому пересмотру. Установка разрешенного программного обеспечения производится либо Администратором лично, либо в присутствии Администратора и под контролем Администратора.

5. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ БЕЗОПАСНОСТИ.

5.1. Под системой регистрации и учета событий безопасности понимается совокупность средств централизованного управления.

5.2. Система регистрации и учета событий безопасности, а также информация, хранящаяся в электронных журналах регистрации событий сами по себе, являются объектами защиты. Администратор принимает меры по защите этой информации в соответствии с техническим заданием на систему защиты информации и системы защиты информации. Доступ к записям системы регистрации и учета событий безопасности разрешен только Администратору.

5.3. Администратор периодически изучает записи системы регистрации и учета событий безопасности и в случае обнаружения инцидентов безопасности информации созывает группу реагирования на инциденты информационной безопасности, которая в свою очередь действует согласно соответствующим инструкциям.

5.4. Реализуется регистрация событий безопасности в виртуальной инфраструктуре. Администратор участвует в настройке системы регистрации событий безопасности в виртуальной инфраструктуре и изучает журналы событий с определенной периодичностью.

- запуск (завершение) работы компонентов виртуальной инфраструктуры;
- доступ субъектов доступа к компонентам виртуальной инфраструктуры;
- изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;
- изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

6. ДЕЙСТВИЯ АДМИНИСТРАТОРА ПРИ РЕМОНТЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ОБСЛУЖИВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И УТИЛИЗАЦИИ НОСИТЕЛЕЙ ИНФОРМАЦИИ.

6.1. Администратор присутствует в процессе установки, обновления, настройки программного обеспечения (в том числе и средств защиты информации) сотрудниками сторонних организаций.

6.2. Администратор присутствует в процессе ремонта технических средств сотрудниками сторонних организаций. Администратор обеспечивает гарантированное затирание данных с носителей информации, либо демонтаж носителей информации (в том числе и оперативной памяти) с технических средств в случае необходимости отправки технических средств для ремонта на территорию сторонних организаций.

6.3. Администратор обеспечивает гарантированное затирание данных на машинных носителях информации при утилизации технических средств, либо принимает участие в физическом уничтожении машинных носителей информации в составе комиссии по уничтожению.

Исполнитель:	Заместитель заведующего		Цуканова А.В.	31.08.2022г.
	(должность)	(подпись)	(Ф.И.О.)	(дата)