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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F6D03A1A8A188D2F86B48B8C01935C94
Владелец: Фокина Светлана Сергеевна
Действителен: с 19.09.2022 до 13.12.2023

УТВЕРЖДЕНО
Заведующий МАДОУ
«Детский сад «Звездочка» г. Белоярский»
_____ /Фокина С.С. /
Приказ № 192 от 31.08.2022 г.

ПЛАН МЕРОПРИЯТИЙ

по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации

г. Белоярский
2022 г.

Разовые мероприятия

№ п/п	Наименование мероприятия	Примечание
1.	Назначение ответственных за защиту информации в или: Создание подразделения по защите информации	
2.	Анализ актуальных угроз безопасности информации и разработка документа «Модель угроз», содержащего, в том числе модель, нарушителя	
3.	Формирование группы реагирования на инциденты информационной безопасности	
4.	Разработка и утверждение инструкции по реагированию на инциденты информационной безопасности	
5.	Разработка и утверждение правил использования средств криптографической защиты информации	
6.	Разработка и утверждение инструкции пользователя, содержащей: • общие обязанности пользователя по защите информации; • правила управления идентификаторами, учетными записями и паролями; • противодействие методам социальной инженерии и правила работы с электронной почтой; • правила работы со съемными носителями информации	
7.	Разработка и утверждение политики информационной безопасности, содержащей: • перечень сведений конфиденциального характера, обрабатываемых; • описание технологических процессов обработки защищаемой информации в информационных системах; • правила и процедуры идентификации и аутентификации пользователей информационных систем; • правила разграничения доступа к ресурсам информационных систем; • правила и процедуры управления информационными потоками; • правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения; • правила защиты машинных носителей информации, контроля интерфейсов ввода-вывода и гарантированного уничтожения информации; • регламент использования и контроля технологий беспроводного доступа и правила защиты беспроводных соединений; • правила взаимодействия информационных систем с внешними информационными системами; • правила и процедуры обеспечения доверенной загрузки средств вычислительной техники; • правила и процедуры применения удаленного доступа к информационным системам; • правила и процедуры обнаружения (предотвращения) вторжений; • правила и процедуры выявления, анализа и устранения уязвимостей; • правила и процедуры контроля установки обновлений программного обеспечения; • правила и процедуры контроля состава технических средств, программного обеспечения и средств защиты информации; • правила и процедуры контроля целостности программного обеспечения;	

№ п/п	Наименование мероприятия	Примечание
	• правила и процедуры резервирования технических средств, программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций; • правила использования электронной почты и защиты от спама; • правила и процедуры контроля использования технологий мобильного кода; • ролевую систему доступа к ресурсам информационных систем; • перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами информационных систем; • перечень лиц, допущенных в помещения, в которых производится обработка конфиденциальной информации; • перечень статических сетевых маршрутов; • список разрешающих правил взаимодействия с внешними телекоммуникационными сетями; • список разрешенного программного обеспечения.	
8.	Организация контролируемой зоны и утверждение положения «О контролируемой зоне»	
9.	Закупка необходимых сертифицированных средств защиты информации	
10.	Реализация проекта системы защиты информации (установка и настройка средств защиты информации)	

Контролирующие и периодические мероприятия

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
1.	Пересмотр актуальных угроз безопасности и актуализация документа «Модель угроз безопасности информации»	Администратор безопасности	Вручную	Ежегодно, либо при изменении нормативной документации в сфере моделирования угроз безопасности информации, либо при поступлении информации о новых угрозах, актуальных для информационных систем	
Информирование и обучение персонала					
2.	Доведение до персонала информации о новых угрозах информационной безопасности	Администратор безопасности	Устные лекции, информирование по каналам электронной почты	Ежеквартально	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
3.	Доведение до персонала положений внутренних нормативных документов по защите информации	Администратор безопасности, Ответственный за информационную безопасность	Устно	По мере появления новых внутренних документов или по мере существенного изменения старых	
4.	Повышение квалификации и переподготовка лиц, ответственных за защиту информации на курсах по направлению «Информационная безопасность» (не менее 72 часов)	Администратор безопасности, Ответственный за информационную безопасность	Планирование учебных курсов	Не реже 1 раза в 5 лет	Учебные курсы должны быть согласованы со ФСТЭК России
5.	Проверка осведомленности персонала в сфере защиты информации	Администратор безопасности, Ответственный за информационную безопасность	Устный опрос, письменное тестирование, имитация действий злоумышленника	Ежеквартально	
Физический контроль					
6.	Осмотр серверного помещения и шкафов с коммутационным оборудованием на предмет несанкционированного доступа, нарушения пломб, физического воздействия и внедрения неучтенных технических средств	Администратор безопасности	Визуальный осмотр	Ежеквартально	
7.	Выборочный осмотр рабочих мест пользователей на предмет несанкционированного доступа, нарушения пломб, физического воздействия и внедрения неучтенных технических средств	Администратор безопасности	Визуальный осмотр	Ежеквартально	
Тестирование работоспособности средств защиты информации					

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
8.	Контроль актуальности антивирусных баз	Администратор безопасности	Kaspersky Security Center	Ежеквартально	
9.	Контроль корректной работы запрещающих правил межсетевого экрана	Администратор безопасности	Браузер, командная строка	Ежеквартально	
10.	Контроль работоспособности средств доверенной загрузки путем имитации попыток загрузки технического средства со стороннего носителя	Администратор безопасности	Загрузочный USB-накопитель	Ежеквартально	
11.	Контроль корректной работы подсистемы гарантированного уничтожения информации	Администратор безопасности	Утилиты восстановления удаленной информации (R.Saver и аналоги)	Ежеквартально, либо при передаче учтенных съемных носителей между пользователями, либо при утилизации/передаче на ремонт технических средств с машинными носителями информации	
Контроль программного обеспечения и технических средств ИС					
12.	Контроль отсутствия у пользователей на рабочих местах средств разработки и технологий интерпретации мобильного кода (кроме пользователей, которым это необходимо для выполнения своих должностных обязанностей)	Администратор безопасности	XSpider 7.8.24, ручной выборочный контроль	Ежеквартально	
13.	Контроль наличия необходимых обновлений безопасности общесистемного и прикладного программного обеспечения	Администратор безопасности	XSpider 7.8.24, ручной выборочный контроль	Ежеквартально	
Пользователи, учетные записи, парольная политика					
14.	Заведение, удаление учетных записей пользователей. Наделение,	Администратор безопасности	Вручную	По мере поступления заявок на заведение/удаление	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	лишение, изменение полномочий пользователей по доступу к ресурсам			учетных записей и наделение/изменение полномочий в системе	
15.	Смена собственного пароля и мониторинг своевременной смены паролей других привилегированных пользователей	Администратор безопасности	Вручную	Ежеквартально	
16.	Смена паролей доступа к интерфейсам управления сетевыми устройствами (коммутаторами, маршрутизаторами)	Администратор безопасности	Вручную	Ежеквартально	
Беспроводные каналы передачи данных					
17.	Мониторинг настроек беспроводных точек доступа на предмет включенных уязвимых функций	Администратор безопасности	Вручную	Ежеквартально	
18.	Мониторинг доступности беспроводного сигнала за пределами контролируемой зоны	Администратор безопасности	Любое мобильное устройство с модулями беспроводной связи	Ежеквартально	
19.	Мониторинг отсутствия поддельных точек доступа, маскирующихся под легальные точки доступа	Администратор безопасности	Любое мобильное устройство с модулями беспроводной связи	Ежеквартально	
Отказоустойчивость					
20.	Резервное копирование информации	Администратор безопасности	вручную	В соответствии с утвержденной политикой информационной безопасности	
21.	Контроль целостности резервных копий	Администратор безопасности	-	Ежеквартально	

Исполнитель: Заместитель заведующего Цуканова А.В. 31.08.2022г.

(должность) (подпись) (Ф.И.О.) (дата)