УТВЕРЖДЕНО
Приказом МДОУ ДС «Морошка»
№ 23 - ОД от 18.11.2022 г.

ПОЛОЖЕНИЕ
о порядке выявления и реагирования на инциденты информационной безопасности в муниципальном дошкольном образовательном учреждение детский сад «Морошка»

Приложение **№ 7**
к приказу № 23 - ОД от 18.11.2022г.

ПОЛОЖЕНИЕ
о порядке выявления и реагирования на инциденты информационной безопасности в Муниципальном дошкольном образовательном учреждение детский сад «Морошка»

1. Общие положения

1.1. Настоящее Положение о порядке выявления и реагирования на инциденты информационной безопасности (далее - Положение) устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационной системы персональных данных Муниципального дошкольного образовательного учреждения детский сад «Морошка» (далее - МДОУ) и (или) возникновению угроз безопасности конфиденциальной информации МДОУ (далее -инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима служебной тайны (далее - служебное расследование) в МДОУ.

1.2. Настоящее Положение распространяется на сотрудников МДОУ.

1.3. Процесс управления инцидентами ИБ включает:

- учет и регистрацию инцидентов ИБ;
- оповещение ответственного лица о возникновении инцидентов ИБ;
- расследование обнаруженных инцидентов ИБ;
- устранение причин и последствий инцидентов ИБ;
- определение плана корректирующих и превентивных мероприятий.

1.4. Требования настоящего Положения являются обязательными для выполнения всеми сотрудниками Департамента образования.

2. Учет и регистрация инцидентов информационной безопасности

2.1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем Департамента образования.

2.2. В обязательном порядке должны регистрироваться следующие события безопасности:

- попытки входа (выхода) пользователей в операционную систему (из операционной системы);
- загрузка и инициализация операционной системы рабочих станций и серверов;
- попытка доступа к средствам виртуализации;
- факт изменения конфигурации средств виртуализации;
- запуск и остановка служб (системных сервисов) средств виртуализации;
- попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

2.3. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

- тип события;
- дата и время события;
- результат события;
- источник события;

- идентификатор пользователя информационной системы, предъявленный при попытке доступа.

2.4. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

2.5. Учет инцидентов ИБ осуществляется администратором безопасности информации (далее- АБИ), назначенным приказом МДОУ. Допускается ведение учета инцидентов ИБ в электронном виде.

2.6. При обнаружении инцидента ИБ АБИ проводит его классификацию в соответствии с Приложением к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

информации;

– по внесению изменений и улучшений в комплект организационно-распорядительной документации по защите персональных данных МДОУ;

– по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

2.7. В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.

2.8. Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами МДОУ.

3. Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности

3.1. Средства защиты информации должны обеспечивать возможность информирования администратора безопасности информации о критических событиях безопасности в информационной системе по электронной почте или посредством смс.

3.2. В случае если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», АБИ обязан незамедлительно сообщить о выявленном инциденте ИБ ответственному по защите информации по электронной почте или иному средству связи.

3.3. Ответственный по защите информации должен провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным данным Положением.

4. Порядок расследования обнаруженных инцидентов информационной безопасности

4.1. Проведение служебного расследования инициируется ответственным за организацию обработки персональных данных МДОУ и осуществляется комиссией по защите персональных данных в МДОУ (далее -Комиссия).

4.2. Служебное расследование может быть возбуждено по:

– решению заведующего МДОУ;

– инициативе любого сотрудника МДОУ на основании служебной записки в произвольной форме на имя ответственного за организацию обработки персональных данных МДОУ;

– устному докладу ответственного по защите информации.

4.3. В состав Комиссии входят следующие сотрудники МДОУ:

4.3.1. в обязательном порядке:

– Председателя Комиссии - ответственного за организацию обработки персональных данных МДОУ;

– Заместителя председателя Комиссии;

– Секретаря Комиссии;

– Членов Комиссии;

- Ответственного по защите информации;
- Администратора безопасности информации;

4.3.2. в случае необходимости Комиссия вправе привлекать к расследованию:

- сотрудников управления информационных технологий и связи; руководителя структурного подразделения, в котором произошел инцидент ИБ;
- непосредственного руководителя сотрудника, в отношении которого проводится служебное расследование;
- экспертов из других структурных подразделений МДОУ и, при необходимости, представителей сторонних организаций.

4.3.3. Комиссия для проведения служебного расследования в рабочем порядке в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное расследование.

4.4. Результаты работы Комиссии оформляются в виде аналитического экспертного заключения - протокола Комиссии на начальника МДОУ, с предложениями:

- по внесению изменений в организационные и (или) технические меры по защите.

5. Ответственность

5.1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный по защите информации.

5.2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор безопасности информации.

Приложение
к Положению о порядке выявления
и реагирования на инциденты
информационной безопасности
в МДОУ ДС «Морошка»

Перечень
инцидентов информационной безопасности

№ п/п	Описание инцидента информационной безопасности
1	2
	1. Текущие нарушения
1.1	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная)
1.2	Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам
1.3	Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры МДОУ
1.4	Выполнение обязанностей с использованием компьютерного производственных оборудования в нерабочее время
1.5	Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
1.6	Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания
1.7	Нецелевое использование элементов информационной инфраструктуры МДОУ (печать, сервисы сети Интернет, электронная почта, и т.п.)
	2. Значимые нарушения
2.1	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная)
2.2	Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
2.3	Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации
2.4	Утрата носителя информации с резервной копией
2.5	Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная)
2.6	Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.)
2.7	Нерегламентированная очистка журналов событий безопасности информационных систем МДОУ
2.8	Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации
2.9	Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования
2.10	Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет
2.11	Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах МДОУ

2.12	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем МДОУ (повышение уровня прав доступа, получение прав на отладку программ и т.п.)
2.13	Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное)
2.14	Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения
2.15	Нерегламентированное использование анализаторов протоколов (снифферов)
2.16	Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите)
2.17	Несанкционированное проведение обновления версий системного и прикладного программного обеспечения
3. Нарушения, имеющие признаки преступления	
3.1	Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры МДОУ
3.2	Несанкционированное изменение конфигурации элементов информационной инфраструктуры МДОУ
3.3	Утрата резервных копий
3.4	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5	Подозрение в умышленном нарушении работоспособности информационной сети МДОУ, элементов информационной инфраструктуры МДОУ, системного и прикладного программного обеспечения
3.6	Юридически не обоснованная передача (распространение) конфиденциальной информации
3.7	Несанкционированное внесение изменений в базы данных информационных систем МДОУ
3.8	Несанкционированное уничтожение конфиденциальной информации
3.9	Проведение обновления версии информационных систем МДОУ (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации
3.10	Намеренное заражение информационных систем МДОУ вредоносным кодом