Муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад комбинированного вида №26»
(МБДОУ ДС №26)

ул. Кирова, 5, г. Озерск Челябинской области, 456780, телефон/факс 8(35130)6-50-09
Сайт: http://sad26-ozr.my1.ru, эл. почта: mbdou-ds26@yandex.ru
ОКПО 53823397, ОГРН 1027401179838, ИНН/КПП 7422025983/741301001

УТВЕРЖДЕНО:
приказом заведующего
МБДОУ ДС № 26
от 25.12.2015 № 350

Положение
о порядке выявления и реагирования
на инциденты информационной безопасности в
Муниципальном бюджетном дошкольном образовательном учреждении
«Детский сад комбинированного вида № 26»
(МБДОУ ДС № 26)

1. Общие положения

1.1. Настоящее Положение устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационной системы МБДОУ ДС № 26 и (или) возникновению угроз безопасности конфиденциальной информации учреждения (далее – инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима коммерческой тайны (далее – служебное расследование) в учреждении.

1.2. Настоящее Положение разработано в соответствии с Положением по организации и проведению работ по обеспечению безопасности конфиденциальной информации при ее обработке в информационной системе МБДОУ ДС № 26. Процесс управления инцидентами ИБ включает:

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

1.3. Требования настоящего Положения являются обязательными для выполнения всеми работниками учреждения.

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 защищенности информационных систем учреждения.

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 и ее программного останова для 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, предъявляемый при попытке доступа.

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

2.5. Учет инцидентов ИБ осуществляется администратором информационной безопасности ИБ осуществляется администратором информационной безопасности информационных систем (далее – администратор ИБ), назначенным приказом по учреждению. Допускается ведение учета инцидентов ИБ в электронном виде.

2.6. При обнаружении инцидента ИБ администратор ИБ проводит его квалификацию в соответствии с приложением № 1 к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

3. Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности

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

В случае, если зафиксированный инцидент ИБ был квалифицирован как «значимый» или «имеющий признаки компьютерного преступления», администратор ИБ обязан незамедлительно сообщить о выявленном инциденте ИБ ответственному за обеспечение безопасности конфиденциальной информации по электронной почте или иному средству связи.

Ответственный за обеспечение безопасности конфиденциальной 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

Проведение служебного расследования инициируется приказом заведующего. В этом же приказе устанавливается состав Комиссии для проведения служебного расследования (далее – Комиссия).

Служебное расследование может быть возбуждено:

- по решению заведующего;
- по инициативе любого работника Администрации округа на основании служебной записки в произвольной форме на имя заведующего;
- по устному докладу заведующего.

В состав Комиссии входят следующие работники учреждения:

4.1.1. В обязательном порядке:

- председатель Комиссии – ответственный за обеспечение безопасности конфиденциальной информации;
- администратор ИБ.

4.1.2. В случае необходимости Комиссия вправе привлекать к расследованию:

- администратора информационных систем Управления образования;
- непосредственного руководителя работника, в отношении которого проводится служебное расследование;
- экспертов из представителей сторонних организаций.

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

Результаты работы комиссии оформляются в виде аналитического экспертного заключения на имя заведующего ДОУ, с предложениями:

- по внесению изменений в организационные и (или) технические меры по защите конфиденциальной информации;
- по внесению изменений и улучшений в комплект организационно-распорядительной документации учреждения;
- по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ.

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 учреждения.

5. Устранение причин и последствий инцидентов информационной безопасности

5.1. Для инициирования работ по устранению причин и последствий инцидентов ИБ ответственный за обеспечение безопасности конфиденциальной информации направляет аналитическое экспертное заключение по электронной почте главе округа и ответственным за выполнение запланированных работ.

Если ответственный за выполнение запланированных работ не согласен с установленными сроками, он вправе обратиться к ответственному за обеспечение безопасности конфиденциальной информации с просьбой перенести срок с обоснованием причин переноса.

При изменении сроков реализации действий, ответственный за обеспечение безопасности конфиденциальной информации вносит необходимые изменения в экспертное заключение и информирует о них по электронной почте ответственного за выполнение запланированных работ, не позднее срока реализации, установленного в экспертном заключении.

5.2. После реализации запланированных работ ответственное лицо должно направить по электронной почте ответственному за обеспечение безопасности конфиденциальной информации подтверждение выполнения работ, не позднее срока реализации, установленного в экспертном заключении.

5.3. Ответственный за обеспечение безопасности конфиденциальной информации вправе запросить у назначенного лица информацию о выполнении в случае, если ему не поступило подтверждение выполнения работ в течение 2 (двух) рабочих дней с даты, установленной в экспертном заключении.

5.4. Оценку результативности предпринятых мер осуществляет ответственный за обеспечение безопасности конфиденциальной информации ежемесячно на основании анализа информации, содержащейся в отчетах о проведении служебного расследования и в свободном отчете об инцидентах ИБ.

5.5. О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

6. Определение плана корректирующих и превентивных мероприятий

Ежемесячно администратор ИБ готовит сводный отчет по инцидентам ИБ, предоставляемый ответственному за обеспечение безопасности конфиденциальной информации ДОУ.

В сводном отчете администратор ИБ должен провести анализ выявленных инцидентов ИБ, в качестве приложения к отчету должен быть предложен перечень корректирующих и превентивных мероприятий, направленных на устранение причин и последствий инцидентов ИБ и на предотвращение подобных нарушений в будущем. Данный перечень должен устанавливать сроки реализации и ответственных за проведение указанных мероприятий.

После согласования указанного перечня с ответственным за обеспечение безопасности конфиденциальной информации, данная информация доводится администратором ИБ до всех работников, назначенных ответственными за проведение корректирующих и превентивных мероприятий.

Контроль за своевременным и качественным выполнением работ по проведению корректирующих и превентивных мероприятий осуществляет ответственный за обеспечение безопасности конфиденциальной информации.

7. Ответственность

7.1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный за обеспечение безопасности конфиденциальной информации.

7.2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор ИБ, назначенный распоряжением заведующего.

Приложение № 1
к Положению о порядке выявления и реагирования
на инциденты информационной безопасности

ПЕРЕЧЕНЬ
инцидентов информационной безопасности МБДОУ ДС № 26

№ п/п	Описание инцидента информационной безопасности
	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 учреждения
1.4.	Выполнение производственных обязанностей с использованием компьютерного 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 отклонения питания
1.7.	Нецелевое использование элементов информационной инфраструктуры учреждения (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)
	Описание инцидента информационной безопасности
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 учреждения
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-носителе или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.д.) и других сервисов сети Интернет
2.11.	Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах учреждения

2.12.	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем учреждения (повышения 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 учреждения
3.2.	Несанкционированное изменение конфигурации элементов информационной инфраструктуры учреждения
3.3.	Утрата резервных копий
Описание инцидента информационной безопасности	
3.4.	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5.	Подозрение в умышленном нарушении работоспособности информационной сети учреждения, элементов информационной инфраструктуры учреждения, системного и прикладного программного обеспечения
3.6.	Юридически необоснованная передача (распространение) конфиденциальной информации
3.7.	Несанкционированное внесение изменений в базы данных информационных систем учреждения
3.8.	Несанкционированное уничтожение конфиденциальной информации
3.9.	Проведение обновления версии информационных систем учреждения (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации
3.10.	Намеренное заражение информационных систем учреждения вредоносным кодом