Муниципальное бюджетное образовательное учреждение средняя общеобразовательная школа с. Исимово Кугарчинского района Республики Башкортостан

ПОРЯДОК

выявления и реагирования на инциденты информационной безопасности

1. Общие положения

1.1. Настоящий Порядок устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационной системы МБОУ СОШ с. Исимово (далее – Учреждение) и (или) возникновению угроз безопасности конфиденциальной информации и персональных данных Учреждения (далее - инциденты ИБ и ПДн), а также регулирует порядок проведения служебного расследования нарушений режима коммерческой тайны (далее – служебное расследование) в Учреждении.

1.2. Процесс управления инцидентами ИБ и ПДн и ПДн включает:

1. учет и регистрацию инцидентов ИБ и ПДн И ПДн;
2. оповещение ответственного лица о возникновении инцидентов ИБ и ПДн и ПДн;
3. расследование обнаруженных инцидентов ИБ и ПДн и ПДн;
4. устранение причин и последствий инцидентов ИБ и ПДн и ПДн; 5. определение плана корректирующих и превентивных мероприятий.

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

2. Учет и регистрация инцидентов информационной безопасности

2.1. Для выявления инцидентов ИБ и ПДн 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 Учреждения.

2.2. В обязательном порядке должны регистрироваться следующие события безопасности:

1. попытки входа (выхода) пользователей в операционную систему (из операционной системы);
2. загрузка и инициализация операционной системы и ее программного обеспечения для рабочих станций и серверов;
3. 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:

1. тип события;
2. дата и время события;
3. результат события;

4. источник события;
5. идентификатор пользователя информационной системы, предъявленный при попытке доступа.

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

2.5. Учет инцидентов ИБ и ПДн осуществляется ответственным за организацию обработки ПДн (далее – ответственный). Допускается ведение учета инцидентов ИБ и ПДн в электронном виде.

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

3. Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности

3.1. В случае, если зафиксированный инцидент ИБ и ПДн был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», ответственный обязан незамедлительно сообщить о выявленном инциденте в МКУ «ГЦИТ «Цитадель»

3.2. Уполномоченный сотрудник МКУ «ГЦИТ «Цитадель» ИБ должен провести внеплановый анализ выявленного инцидента ИБ и ПДн 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 приказом директора Учреждения. В этом же приказе устанавливается состав Комиссии для проведения служебного расследования (далее – Комиссия) с обязательным привлечением уполномоченных сотрудников МКУ «ГЦИТ «Цитадель».

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

4.3. Результаты работы Комиссии оформляются в виде аналитического экспертного заключения на имя директора Учреждение, с предложениями:

1. по внесению изменений в организационные и (или) технические меры по защите конфиденциальной информации;
2. по внесению изменений и улучшений в комплект организационнораспорядительной документации Учреждения;
3. по расширению или дополнению списка инцидентов ИБ и ПДн, установленного данным Положением, если это необходимо.

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

5.1. Ответственность за обеспечение своевременной регистрации инцидентов ИБ и ПДн, проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный.

Приложение
к Порядку выявления и реагирования на инциденты
информационной безопасности

Перечень инцидентов информационной безопасности Учреждения

№ 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.	Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
1.5.	Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания
1.6.	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)
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-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 Учреждения
2.12.	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем Учреждения (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 Учреждения
3.2.	Несанкционированное изменение конфигурации элементов информационной инфраструктуры Учреждения
3.3.	Преднамеренная утрата резервных копий.
3.4.	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5.	Подозрение в умышленном нарушении работоспособности информационной сети Учреждение, 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