Принято на Совете ОУ
Протокол № _1_
от « 20 » октября 2017г.

УТВЕРЖДЕНО
Приказом директора
МКОУ СОШ с.Слудка
№ 63 от « 24 » октября 2017г.

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в МКОУ СОШ с. Слудка (в новой редакции)

1. Общие положения

1.1. Настоящий Регламент реагирования на инциденты информационной безопасности (далее – Регламент) устанавливает порядок действий лиц, ответственных за обеспечение информационной безопасности в МКОУ СОШ с.Слудка (далее – Учреждение или администратор ИБ), при выявлении инцидента информационной безопасности в целях снижения его негативных последствий, а также порядок проведения расследования инцидента информационной безопасности (далее – инцидент).

1.2. Настоящий регламент разработан с учетом ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

1.3. Руководство действиями, предусмотренными данным Регламентом, осуществляет лицо, ответственное за обеспечение информационной безопасности в Учреждении.

2. Реагирование на инциденты информационной безопасности

2.1. Понятие «инцидент информационной безопасности» – это одно или серия событий, которое привело к уничтожению, модификации, копированию, распространению (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах Учреждения, а также блокировке доступа к ней.

Инциденты могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами (приложение №1).

Следует отличать событие информационной безопасности от инцидента. Событие информационной безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение принятых организационно-распорядительных документов по защите информации или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Событие может быть результатом случайных или преднамеренных попыток компрометации защитных мер, но в большинстве случаев событие само по себе не означает, что попытка в действительности была успешной и, следовательно, каким-то образом повлияла на конфиденциальность, целостность и (или) доступность, то есть не все события будут отнесены к категории инцидентов.

2.2. Выявление инцидента

Основными источниками, от которых администратор ИБ может получить сведения об инцидентах информационной безопасности, являются:

сообщения от работников Учреждения о выявленных фактах нарушения информационной безопасности*;*

результаты работы средств мониторинга информационной безопасности,

результаты проверок и аудита (внутреннего или внешнего);

журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем и средств защиты информации.

Администратор ИБ должен регулярно информировать работников о необходимости немедленного его оповещения о возникновении инцидента с указанием контактной информации и способов предоставления информации.

2.3. Порядок действий администратора ИБ при обнаружении инцидента информационной безопасности

2.3.1. Анализ исходной информации и принятие решения о проведении разбирательства Администратор ИБ с момента получения информации о предполагаемом инциденте информационной безопасности незамедлительно проводит первоначальный анализ полученных данных.

По усмотрению администратора ИБ в случае если инцидент не привел к негативным последствиям в связи с уничтожением, модификацией, копированием, распространением (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах, а также блокировке доступа к ней (например, случайное удаление файлов с информацией, имеющей резервные копии, не имеет негативных последствий для деятельности в Учреждении разбирательство может не проводиться.

В случае если инцидент привел к негативным последствиям, администратор ИБ собирает группу реагирования на инциденты информационной безопасности в целях совместного принятия решения о необходимости проведения разбирательства. В группу включаются компетентные сотрудники в области информационных технологий в Учреждении.

В случае принятия группой решения о необходимости проведения разбирательства администратор ИБ информирует об инциденте информационной безопасности директора Учреждения.

2.3.2. Реагирование на инцидент информационной безопасности (устранение причин и последствий инцидента) Администратор ИБ совместно с группой реагирования на инциденты информационной безопасности по согласованию с директором Учреждения определяет и в кратчайшие сроки, не превышающие одного рабочего дня, инициирует первоочередные меры, направленные на локализацию инцидента и минимизацию его последствий.

В случае если инцидент информационной безопасности связан с совершением компьютерных атак или внедрением вредоносного программного обеспечения, администратор ИБ в целях совместной выработки и реализации мер по их локализации, устранению и ликвидации последствий должен незамедлительно информировать:

головное подразделение по технической защите информации, не содержащей сведений, составляющих государственную тайну (министерство информационных технологий и связи Кировской области), тел. 8 (8332) 27-90-24 (в рабочее время);

дежурную службу Управления ФСБ России по Кировской области, тел. 8 (8332) 35-81-11 (круглосуточно), e-mail: kirov@fsb.ru;

дежурную смену Регионального центра мониторинга компьютерных атак Управления ФСБ России по Нижегородской области, тел. 8 (831) 439-88-86 (круглосуточно), e-mail: rcm4@rcm4.ru.

2.3.3. Разбирательство (проведение служебного расследования) инцидента информационной безопасности

После локализации инцидента и восстановления штатного режима работы проводится разбирательство инцидента информационной безопасности.

Разбирательство представляет собой получение (сбор) необходимой информации об инциденте, доказательств факта возникновения инцидента, определение обстоятельств (деталей), способствовавших совершению инцидента, в целях определения причин возникновения инцидента, виновных лиц и меры ответственности за нарушение безопасности информации.

Важным является обеспечение сохранности и целостности доказательств факта возникновения инцидента для их представления на судебном процессе при необходимости привлечения лица, по вине которого произошел инцидент, к ответственности в соответствии с действующим законодательством Российской Федерации.

По результатам расследования администратор ИБ формирует заключение по расследованию инцидента, согласовывает его со всеми участниками разбирательства и передает имеющиеся материалы (в объеме, достаточном для принятия решения)

директору учреждения для решения вопроса о привлечении виновного в инциденте к ответственности.

2.3.4. Порядок документирования процедур

На основе собранной в процессе разбирательства информации администратор ИБ также заполняет отчет об инциденте (приложение № 2) в целях систематизации информации об инцидентах и ее дальнейшего анализа. В отчете указывается следующая информация:

1. Дата и время совершения инцидента.

2. Источник информации, от которого администратор ИБ получил информацию об инциденте (в соответствии с п. 2.2 настоящего регламента).

3. Ф.И.О. и должность лица, по вине которого произошел инцидент.

Если инцидент произошел по причине некорректной работы средств защиты информации или их некорректной настройки, ответственность за инцидент несет лицо, ответственное за установку, настройку и функционирование средств защиты информации.

Если инцидент произошел по причине некорректной работы программного обеспечения или технических средств, ответственность несут лицо, ответственное за функционирование программного обеспечения и технических средств.

В случае если инцидент произошел вследствие невыполнения работниками требований организационно-распорядительных документов по защите информации учреждения, персональную ответственность несут работники, нарушившие требования документов, в том числе работники, на которых возложен контроль соблюдения требований данных документов.

4. Описание инцидента.

В качестве примера описания инцидента можно рассмотреть приложение № 1 к настоящему Регламенту.

Также в данном разделе необходимо указать какое из свойств информации было нарушено (конфиденциальность, целостность, доступность) в результате инцидента и указать функциональное воздействие инцидента на деятельность учреждения:

несущественный – воздействие на способность учреждением выполнять свои функции отсутствует;

низкий – минимальный эффект, учреждение все еще может выполнять все основные функции, но со сниженной эффективностью;

средний – учреждение потеряла способность обеспечить часть основных функции;

высокий – учреждение не в состоянии выполнять свои функции.

5. Причины инцидента.

6. Меры, принятые для устранения причин, последствий инцидента.

Данный пункт позволит в случае повторного возникновения инцидента в минимальные сроки устранить его. По результатам формирования отчета об инциденте администратором ИБ заполняется Журнал учета инцидентов информационной безопасности (приложение № 3).

Журнал позволяет вести статистику всех инцидентов информационной безопасности, которая является показателем эффективности функционирования системы защиты информации. Статистику инцидентов следует регулярно анализировать в рамках проведения оценки защищенности информационных систем.

2.3.5. Выработка корректирующих и превентивных мероприятий

По результатам разбирательства принимается решение о необходимо предотвращение или минимизацию рисков возникновения подобных нарушений в будущем (в некоторых случаях последствия инцидента незначительны по сравнению с корректирующими и превентивными действиями, и тогда целесообразно не совершать дальнейших шагов после устранения последствий инцидента).

3. Ответственность

Каждый работник учреждения несет персональную дисциплинарную, административную или уголовную ответственность за действия либо бездействия, повлекшие неправомерное уничтожение, блокирование, модификацию либо копирование информации, в соответствии с действующим законодательством Российской Федерации.

Приложение № 1

ПЕРЕЧЕНЬ
инцидентов информационной безопасности

№	Описание инцидента информационной безопасности
1	Утрата (кража) магнитного, оптического или иного носителя съемного носителя конфиденциальной информации
2	Разглашение конфиденциальной информации
3	Утечка конфиденциальной информации
4	Утрата идентификационной информации (логина и пароля)
5	Нерегламентированная передача конфиденциальной информации по сети «Интернет» по электронной почте, с использованием сервисов мгновенных сообщений, иных сервисов
6	Неоднократное оставление работающего (включенного) компьютерного оборудования без блокировки экрана монитора
7	Нарушение или сбои в работе системы резервного копирования, утрата резервных копий
8	Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (намеренное, непреднамеренное)
9	Несанкционированное изменение (модификация), уничтожение информации
10	Выход из строя машинного носителя информации (флэш-накопители, внешние накопители на жестких дисках машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках)),
11	Выход из строя, нарушение функционирования технических средств
12	Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам
13	Ошибка при регистрации в информационной системе: ввод неправильных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная, многократная)
14	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем (повышение уровня прав доступа, получение прав на отладку программ и т.п.)
15	Подключение неучтенных внутренних и (или) периферийных устройств и носителей информации
16	Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные
17	Несанкционированное проведение обновления версий системного и прикладного программного обеспечения
18	Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования
19	Нерегламентированная очистка журналов событий безопасности

Приложение № 2

ОТЧЕТ
об инциденте информационной безопасности № ____
(номер вносится в журнал)

Инцидент зафиксирован
_____
(дата, фамилия и инициалы работника (-ов))
В инциденте задействованы следующие работники
_____
(фамилия и инициалы работника (-ов))
_____
Описание инцидента
_____
_____
_____
_____
Причины инцидента
_____
_____
_____
Меры, принятые для устранения причин, последствий инцидента
_____
_____
_____
_____

<Администратор ИБ,
указывается должность> *Фамилия И.О.*
«___» _____ 201__ г.

Приложение № 3

Журнал
учета инцидентов информационной безопасности
на ____ листах

начат «___»_____20__г.
окончен «___»_____20__г.

Ответственный за ведение журнала

_____ _____ _____ _____
Должность Ф.И.О. дата подпись

№	№ отчета об инциденте	Дата совершения инциденте	Краткое описание инцидента (заражение вирусом, компьютерная атака, утечка информации, сбой в работе оборудования и проч.)	Сроки устранения инцидента	Подпись лица, зарегистрировавшего инцидент в журнале