

УТВЕРЖДАЮ

Директор школы



Т.В. Володина Т.В. Володина

Приказ №17 от «01» марта 2017 г.

РЕГЛАМЕНТ
реагирования на инциденты
информационной безопасности в
Кировском областном государственном
общеобразовательном бюджетном учреждении
«Средняя школа пгт Оричи»

Содержание

1. Назначение настоящего документа.....	2
2. Область действия настоящего документа.....	2
3. Основные положения.....	2
4. Ответственность.....	7

1. Назначение настоящего документа

Настоящий Регламент реагирования на инциденты информационной безопасности (далее – Регламент) устанавливает порядок действий лиц, ответственных за обеспечение информационной безопасности в КОГОбУ СШ пгт Оричи (далее – администратор ИБ), при выявлении инцидента информационной безопасности в целях снижения его негативных последствий, а также порядок проведения расследования инцидента информационной безопасности (далее – инцидент).

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

2. Область действия настоящего документа

Руководство действиями, предусмотренными данным Регламентом, осуществляет лицо, ответственное за обеспечение информационной безопасности в КОГОбУ СШ пгт Оричи (далее – администратор ИБ).

3. Основные положения

3.1. Понятие «инцидент информационной безопасности»

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 в КОГОбУ СШ пгт Оричи, 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.

Примеры инцидентов информационной безопасности приведены в приложении № 1 к настоящему Регламенту.

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.

3.2. Выявление инцидента

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

сообщения от работников в КОГ ОБУ СШ пгт Оричи 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.

3.3. Порядок действий администратора ИБ при обнаружении инцидента информационной безопасности

3.3.1. 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 КОГ ОБУ СШ пгт Оричи) 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 КОГОВУ СШ пгт Оричи.

В случае принятия группой решения о необходимости проведения разбирательства администратор ИБ информирует об инциденте информационной безопасности руководителя в КОГОВУ СШ пгт Оричи.

3.3.2. Реагирование на инцидент информационной безопасности (устранение причин и последствий инцидента)

Администратор ИБ совместно с группой реагирования на инциденты информационной безопасности по согласованию с руководителем в КОГОВУ СШ пгт Оричи 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 КОГОВУ СШ пгт Оричи 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) 358-111 (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.

3.3.3. 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) руководителю в КОГОВУ СШ пгт Оричи для решения вопроса о привлечении виновного в инциденте к ответственности.

3.3.4. 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. 3.2 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 в КОГОВУ СШ пгт Оричи, 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 в КОГОбУ СШ пгт Оричи:

несуществующий – воздействие на способность в КОГОбУ СШ пгт Оричи выполнять свои функции отсутствует;

низкий – минимальный эффект; в КОГОбУ СШ пгт Оричи все еще может выполнять все основные функции, но со сниженной эффективностью;

средний – в КОГОбУ СШ пгт Оричи потеряло способность обеспечить часть основных функций;

высокий – в КОГОбУ СШ пгт Оричи 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.

3.3.5. Выработка корректирующих и превентивных мероприятий

По результатам разбирательства принимается решение о необходимости принятия дополнительных организационных и технических мер, направленных на 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).

4. Ответственность

Каждый работник в КОГОбУ СШ пгт Оричи 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.

**ПЕРЕЧЕНЬ
инцидентов информационной безопасности**

№ п/п	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 сбой 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

№ п/п	Описание инцидента информационной безопасности
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

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>*

« ____ » _____ 201__ г.

Фамилия И.О.

Приложение № 3

к регламенту

ЖУРНАЛ
учета инцидентов информационной безопасности

на _____ листах

Начат « ____ » _____ 20__
Окончен « ____ » _____ 20__

Ответственный за ведение журнала

<должность>	<Ф.И.О.>	<дата>	<подпись>
-------------	----------	--------	-----------

