УТВЕРЖДЕНО

Приказом <НАЗВАНИЕ ДОЛЖНОСТИ>
<НАЗВАНИЕ ОРГАНИЗАЦИИ>

<ФИО>

№____ от «___» _____ 20 ___г.

Инструкция по управлению инцидентами ИБ <НАЗВАНИЕ ОРГАНИЗАЦИИ>

Ярославль, 2015

Оглавление

1. Аннотация

Инструкция по управлению инцидентами ИБ (далее – Инструкция) <ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ> (далее – <СОКРАЩЁННОЕ>) определяет общие функции, ответственность, права и обязанности ответственных за управление инцидентами информационной безопасности лиц.

2. Сокращения

Принятое сокращение	Полное наименование
ГРИИБ	Группа реагирования на инциденты информационной безопасности
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
МЭ	Межсетевой экран
ОС	Операционная система
ТС	Технические средства
ЯО	Ярославская область

3. Термины и определения

Группа реагирования на инциденты ИБ (далее - ГРИБ) – действующая на постоянной основе группа работников <Учреждения>, которая выполняет процедуры менеджмента инцидентов ИБ в течение их жизненного цикла. ГРИБ способствует оперативному реагированию на инциденты ИБ, в том числе за счет независимости применяемых процедур и средств вычислительной техники от компонентов информационной инфраструктуры Учреждения.

Журнал регистрации событий – электронный журнал, содержащий записи о действиях пользователей и событиях в автоматизированной системе.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

Информационная безопасность – состояние защищённости интересов Учреждения.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Инцидент информационной безопасности — Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Событие информационной безопасности — Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Менеджмент инцидентов ИБ – деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них в интересах минимизации и/или ликвидации негативных последствий для Учреждения при нарушениях ИБ.

Событие – возникновение специфического набора обстоятельств.

4. Основания для разработки

Настоящая Инструкция разработана во исполнение требований следующих документов:

- Приказ ФСТЭК России № 17 от 11 февраля 2013 года "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
- Методический документ утвержден ФСТЭК России 11 февраля 2014 г. "Меры защиты информации в государственных информационных системах".

5. Содержание инструкции

5.1. Общие положения

Отслеживание и реагирование на инциденты ИБ осуществляет ГРИИБ.

Все сотрудники < НАЗВАНИЕ ОРГАНИЗАЦИИ> должны немедленно уведомлять администратора ИБ о выявленных слабых местах и инцидентах ИБ. Пользователи не должны использовать имеющиеся уязвимости.

После получения уведомления, а также в случае самостоятельного обнаружения инцидента ИБ администратор ИБ должен отреагировать на инцидент ИБ и принять меры по:

1. Анализу инцидента ИБ.
2. Предотвращению развития инцидента ИБ.
3. Устранению инцидента ИБ.
4. Восстановлению безопасности после инцидента ИБ.
5. Регистрации инцидента ИБ, проведении внутреннего расследования (при необходимости).
6. Формирование рекомендаций по результатам инцидента ИБ по повышению уровня ИБ.

Информация об инцидентах ИБ, приведших к нарушению безопасности ИС, должна быть задокументирована Администратором ИБ в форме «Отчёта об инциденте ИБ» (ПРИЛОЖЕНИЕ)

В <НАЗВАНИЕ ОРГАНИЗАЦИИ> должна осуществляться периодическая проверка эффективности действий по реагированию на инциденты ИБ. Проверка может осуществляться в виде «Тестов на проникновение» в рамках проведения внутреннего или внешнего аудита.

5.2. Выявление инцидентов информационной безопасности

Основными источниками информации об Инцидентах ИБ являются:

1. факты, выявленные отделом <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ>, а также другими сотрудниками организации;
2. результаты работы средств мониторинга ИБ, результаты проверок и аудита (внутреннего или внешнего);
3. журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
4. обращения субъектов персональных данных с указанием Инцидента ИБ;
5. запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;
6. другие источники информации.

Основными видами инцидентов ИБ в <НАЗВАНИЕ ОРГАНИЗАЦИИ> являются:

1. **разглашение конфиденциальной информации**, либо угроза такого разглашения;
2. **несанкционированный доступ** к конфиденциальной информации со стороны лиц, которые не имеют никакого легального доступа к ресурсам или помещениям организации;

3. **превышение полномочий** - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников <НАЗВАНИЕ ОРГАНИЗАЦИИ>;
4. **компрометация учетных записей или паролей**;
5. **вирусная атака** или вирусное заражение;
6. нарушение или **сбой в работе системы резервного копирования**;
7. **нарушение правил использования персональных данных**.

Любые сведения о Событии или Инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником отделу ИБ.

5.3. Выявление инцидентов информационной безопасности

Администратор ИБ отдела <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> после получения информации о предполагаемом Инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа Администратор ИБ проводит проверку наличия в выявленном факте нарушений.

По усмотрению Администратора ИБ единичный Инцидент ИБ, не приведший к негативным последствиям и совершенный сотрудником <НАЗВАНИЕ ОРГАНИЗАЦИИ> впервые, фиксируется отделом <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> в карточке данных «Инциденты ИБ» (приложение №1) с присвоением статуса «Разбирательство не требуется».

В случае наличия признаков Инцидента ИБ, приведшего к негативным последствиям, Администратор ИБ классифицирует инцидент, определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует <Главврача> <НАЗВАНИЕ ОРГАНИЗАЦИИ> об Инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, Администратор ИБ определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

5.4. Разбирательство инцидента информационной безопасности

5.4.1. Цели и этапы разбирательства Инцидента ИБ

Целями разбирательства инцидентов ИБ являются:

1. выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
2. защита прав <НАЗВАНИЕ ОРГАНИЗАЦИИ>, установленных законодательством Российской Федерации;
3. защита информационных ресурсов <НАЗВАНИЕ ОРГАНИЗАЦИИ>;
4. обеспечение безопасности персональных данных;
5. обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых <НАЗВАНИЕ ОРГАНИЗАЦИИ>;
6. предотвращение несанкционированного доступа к конфиденциальной информации, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

Разбирательство Инцидента ИБ, состоит из следующих этапов:

1. подтверждение/опровержение факта возникновения Инцидента ИБ;
2. классификация инцидента ИБ;

3. подтверждение/корректировка уровня значимости Инцидента ИБ;
4. уточнение дополнительных обстоятельств (деталей) Инцидента ИБ;
5. получение (сбор) доказательств возникновения Инцидента ИБ, обеспечение их сохранности и целостности;
6. минимизация последствий Инцидента ИБ;
7. информирование и консультирование сотрудников <НАЗВАНИЕ ОРГАНИЗАЦИИ> по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
8. переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил ИБ.

5.4.2. Порядок проведения разбирательства Инцидента ИБ:

В процессе проведения разбирательства Инцидента ИБ обязательными для установления являются:

1. дата и время совершения Инцидента ИБ;
2. ФИО, должность и подразделение Нарушителя ИБ;
3. классификация инцидента;
4. уровень критичности Инцидента ИБ;
5. обстоятельства и мотивы совершения Инцидента ИБ;
6. информационные ресурсы, затронутые Инцидентом ИБ;
7. характер и размер реального и потенциального ущерба;
8. обстоятельства, способствовавшие совершению Инцидента ИБ.

После получения необходимой информации по Инциденту ИБ осуществляющий разбирательство сотрудник отдела ИБ проводит анализ полученных данных.

С момента выявления инцидента ИБ Администратор ИБ запрашивает у руководителя структурного подразделения объяснительную записку Нарушителя ИБ. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение 3 рабочих дней и представлена отделу <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ>. В случае отказа Нарушителя ИБ предоставить объяснительную записку, сотрудник отдела ИБ составляет акт, составленный в соответствии с установленным в <НАЗВАНИЕ ОРГАНИЗАЦИИ> порядке.

Сотрудник отдела ИБ проводит оценку негативных последствий от реализации Инцидента ИБ. В ходе данной оценки учитываются:

1. прямой финансовый ущерб;
2. репутационный ущерб;
3. потенциальный ущерб;
4. косвенные потери, связанные с недоступностью сервисов, потерей информации;
5. другие виды ущерба или аспекты негативных последствий для <НАЗВАНИЕ ОРГАНИЗАЦИИ> или субъектов персональных данных.

С целью минимизации последствий Инцидента ИБ возможно временное отключение прав доступа сотрудника к Информационным ресурсам на время проведения расследования. Подобное отключение инициируется сотрудником отдела <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> с обязательным предварительным устным согласованием с начальником сотрудника.

5.5. Оформление результатов проведенного разбирательства

Собранная в процессе разбирательства Инцидента ИБ информация фиксируется Администратором ИБ в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по Инциденту ИБ (Приложение).

Администратор ИБ формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию Инцидента ИБ.

Итоговое заключение по Инциденту ИБ Администратор ИБ направляет начальникам отделов, затронутых Инцидентом ИБ.

Администратор ИБ фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

В случае выявления в Инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, сотрудник ИБ передает все материалы по Инциденту ИБ <Главврач> <НАЗВАНИЕ ОРГАНИЗАЦИИ> для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

5.6. Завершение разбирательства, превентивные мероприятия

По завершению разбирательства Инцидента ИБ, Администратор ИБ передает имеющиеся материалы (в объеме, достаточном для принятия решения) начальнику отдела Нарушителя ИБ для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

На основании полученных результатов разбирательства отдел ИБ организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

1. анализ и пересмотр имеющихся прав доступа к информационным ресурсам у Нарушителя ИБ;
2. доведение до всех сотрудников требований внутренних нормативных документов;
3. обсуждение Инцидента ИБ на совещании;
4. отмена неактуальных прав доступа к информационным ресурсам.

6. Права и обязанности

Администратор ИБ имеет право:

- По согласованию с непосредственным начальником Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам Инцидента ИБ у Нарушителя ИБ.
- Запрашивать и получать от начальников и сотрудников <НАЗВАНИЕ ОРГАНИЗАЦИИ>, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента ИБ.
- Инициировать отключение от информационных ресурсов сотрудников <НАЗВАНИЕ ОРГАНИЗАЦИИ, нарушивших правила или требования ИБ, на период проведений расследования Инцидента ИБ в случае если имеется существенный риск того, что продолжение работы сотрудника с ИР может повлечь значительное увеличение ущерба или новые инциденты ИБ.
- Инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной и (или) материальной ответственность согласно внутренним нормативным документам <НАЗВАНИЕ ОРГАНИЗАЦИИ>.

Администратор ИБ обязан:

- Объективно проводить разбирательство каждого Инцидента ИБ.
- Определять первоочередные меры, направленные на локализацию Инцидента ИБ и минимизацию негативных последствий.

- Фиксировать в карточке данных "Инциденты ИБ" всю исходную информацию об Инциденте ИБ и результаты его расследования.
- Предоставлять отчеты и рекомендации по проведенным разбирательствам руководству.
- Проводить анализ обстоятельств, способствовавших совершению каждого Инцидента ИБ, и на его основе, совместно с отделом автоматизации информационного обеспечения, разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных Инцидентов ИБ и минимизации возможности их повторения в будущем.

Сотрудники <НАЗВАНИЕ ОРГАНИЗАЦИИ> обязаны:

- предоставлять по запросам сотрудника отдела <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства Инцидента ИБ;
- информировать отдел <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> о выявленных Инцидентах ИБ.

7. Ответственность

Каждый сотрудник, имеющий доступ в ИС несёт персональную ответственность за обеспечение ИБ в соответствии с требованиями настоящей Инструкции.

Лица, нарушившие требования безопасности, изложенные в настоящей Инструкции могут быть привлечены к дисциплинарной или административной ответственности в соответствии с действующим законодательством Российской Федерации.

8. Контроль и пересмотр

<НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> по мере необходимости, но не реже чем в пять лет, пересматривает настоящую Инструкцию. Изменения и дополнения вносятся по инициативе <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> или <Директора> и утверждаются <Директором>.

Все изменения, внесённые в настоящую Инструкцию должны учитываться в листе «История изменений».

9. История изменений

Версия	Дата утверждения	Изменения	Кто внёс изменения

Приложение 1. Карточка инцидента

Карточка данных об инциденте ИБ № _____

Дата составления:Место для ввода даты.

1. Информация об источнике информации о событии ИБ:

ФИО	
Должность	
Телефон	
Электронная почта	

2. Описание события ИБ

Описание события	
Описание способа реализации:	
Причины события:	
Негативное воздействие:	
Связанные активы:	

3. Дополнительные сведения о событии ИБ:

Дата возникновения события	Место для ввода даты.
Дата обнаружения события	Место для ввода даты.
Дата регистрации события:	Место для ввода даты.
Событие закончилось?	
Продолжительность события:	

Описание Инцидента ИБ

Тип инцидента Выберите элемент.
Преднамеренность Выберите элемент.

Тип угрозы (один из):
☐**Намеренная** Выберите элемент.
☐**Случайная** Выберите элемент.
☐**Ошибка** Выберите элемент.
☐**Неизвестно**

Комментарии:

4. Поражённые активы:

Информация:
Технические средства:
Программное обеспечение:
Каналы связи:
Документация:

Негативное воздействие/влияние инцидента

Свойство ИБ	Нарушение	**Значимость**
Нарушение конфиденциальности (т. е., несанкционированное раскрытие)	☐	
Нарушение целостности (т. е., несанкционированная модификация)	☐	
Нарушение доступности (т. е., недоступность)	☐	

Оценка стоимости восстановления инцидента:

Расследование инцидента

Дата начала расследования инцидента Место для ввода даты.
Дата окончания инцидента Место для ввода даты.
Дата окончания воздействия Место для ввода даты.
Дата завершения расследования: Место для ввода даты.

Предполагаемый нарушитель:

Предпринятые действия:

Рабочая группа:

(должность)

(Ф.И.О.) *(Подпись)* «____» _____ г. *(Дата)*

(должность)

(Ф.И.О.) *(Подпись)* «____» _____ г. *(Дата)*

(должность)

(Ф.И.О.) *(Подпись)* «____» _____ г. *(Дата)*

Приложение 2. Форма отчёта по событию ИБ

Отчёт о событии ИБ № _____

Дата составления:Место для ввода даты.

1. Сводная информация:

№	Дата выявления	Характер события	Дата выявления	Подразделение	Объект инфраструктуры

2. Детальная информация:

(Подробное описание события)

Приложение 3. Форма отчёта об инциденте ИБ

Конфиденциально
(по заполнению)

Отчёт об инциденте ИБ № _____

Дата составления:Место для ввода даты.

3. Сводная информация:

Наименование инцидента	Дата выявления	Подразделение	Статус	Уровень
Выберите элемент.	Место для ввода даты.		Выберите элемент.	Выберите элемент.

4. Детальная информация:

Дата выявления: Место для ввода даты.
Дата совершения: Место для ввода даты.
Дата завершения разбирательства: Место для ввода даты.

Краткое описание инцидента:

5. Подробное описание инцидента

Затронутые подразделения:

Объекты инфраструктуры

Способ реализации: Выберите элемент.

Негативное воздействие: Выберите элемент.

Уровень ущерба: Выберите элемент.

6. Состав рабочей группы:

(должность)

(Ф.И.О.) *(Подпись)* «____» *(Дата)* ____ г.

(должность)

(Ф.И.О.) *(Подпись)* «____» *(Дата)* ____ г.