Утверждаю
Директор ФКПОУ «МЭКИ»
Минтруда России В.Н.Медведев

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в ФКПОУ «МЭКИ» Минтруда России

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов информационной безопасности в ФКПОУ «МЭКИ» Минтруда России (далее – Учреждение).

1.2. Регламент разработан в соответствии с Концепцией информационной безопасности, принятой в Учреждении, Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Федеральным законом от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании" Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" иными нормативными правовыми актами, а также в соответствии с локальными нормативными актами Учреждения.

1.3. Настоящий Регламент обязателен к соблюдению всеми работниками Учреждения, участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности (далее – ИБ).

1.4. Разбирательство по всем инцидентам ИБ проводится ответственным за информационную безопасность с привлечением начальника отдела информатизации и системного администратора, а также руководителей и сотрудников других подразделений.

1.5. Разбирательство инцидентов ИБ, затрагивающих два или более подразделения Учреждения, проводится администратором информационной безопасности с привлечением руководителей соответствующих подразделений.

2. Выявление инцидента информационной безопасности

2.1. Основными источниками информации об Инцидентах ИБ являются:

- факты, выявленные руководителем структурного подразделения Учреждения, лицом назначенным ответственным за информационную безопасность, а также начальником отдела информатизации и системным администратором.
- результаты работы средств мониторинга ИБ, результаты проверок и аудита (внутреннего или внешнего);
- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
- обращения субъектов персональных данных с указанием Инцидента ИБ;
- запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;
- другие источники информации.

2.2. Основными видами инцидентов ИБ в Учреждении являются:

- разглашение конфиденциальной или внутренней информации, либо угроза такого разглашения;
- несанкционированный доступ - доступ лиц, которые не имеют никакого легального доступа к ресурсам или помещениям организации;
- превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников Учреждения;
- компрометация учетных записей или паролей;
- вирусная атака или вирусное заражение;
- нарушение или сбои в работе системы резервного копирования;
- нарушение правил использования персональных данных.

2.3. Работник Учреждения может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации, утвержденными в Учреждении. Выявленные несоответствия дают основания предполагать факт возникновения Инцидента ИБ. Любые сведения о Происшествии или Инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником ответственному за информационную безопасность.

3. Анализ исходной информации и принятие решения о проведения разбирательства

3.1. Ответственный за информационную безопасность после получения информации о предполагаемом Инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа он проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению ответственного за информационную безопасность единичный Инцидент ИБ, не приведший к негативным последствиям и совершенный сотрудником Учреждения впервые, фиксируется администратором ИБ в карточке данных
«Инциденты ИБ» *(приложение №1)* с присвоением статуса «Разбирательство не требуется».

3.4. В случае наличия признаков Инцидента ИБ, приведшего к негативным последствиям, ответственный за информационную безопасность классифицирует инцидент, определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует директора Учреждения либо начальника отдела информатизации об Инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, ответственный за информационную безопасность по согласованию с директором Учреждения определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

4. Разбирательство инцидента информационной безопасности

4.1.Цели и этапы разбирательства Инцидента ИБ:

4.1.1. Целями разбирательства инцидентов ИБ являются:

- выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
- защита прав Учреждения, установленных законодательством Российской Федерации;
- защита репутации Учреждения и ее информационных ресурсов;
- обеспечение безопасности персональных данных;
- обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых Учреждением;
- предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство Инцидента ИБ, состоит из следующих этапов:

- подтверждение/опровержение факта возникновения Инцидента ИБ;
- классификация инцидента ИБ;
- подтверждение/корректировка уровня значимости Инцидента ИБ;
- уточнение дополнительных обстоятельств (деталей) Инцидента ИБ;

- получение (сбор) доказательств возникновения Инцидента ИБ, обеспечение их сохранности и целостности;
- минимизация последствий Инцидента ИБ;
- информирование и консультирование персонала Учрежденния по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
- переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил ИБ.

4.2. Порядок проведения разбирательства Инцидента ИБ:

4.2.1. 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.

4.2.2. При Инциденте ИБ, затрагивающем не более одного структурного подразделения, ответственный за информационную безопасность информирует о факте инцидента руководителя соответствующего структурного подразделения.

4.2.3. При Инциденте ИБ, затрагивающим более одного структурного подразделения, ответственный за информационную безопасность информирует руководителей соответствующих подразделений и инициирует проведение разбирательства.

4.2.4. В случае проведения временного отключения прав доступа у предполагаемого Нарушителя ИБ информация об отключении прав доступа направляется руководителю предполагаемого Нарушителя ИБ.

4.2.5. Осуществляющий разбирательство ответственный за информационную безопасность в процессе проведения расследования Инцидента ИБ при необходимости запрашивает информацию в структурных подразделениях, запрос направляется на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.2.6. После получения необходимой информации по Инциденту ИБ осуществляющий разбирательство ответственный за информационную безопасность проводит анализ полученных данных,

4.2.7. В течение 5 (пяти) рабочих дней с момента выявления инцидента ИБ ответственный за информационную безопасность запрашивает у руководителя структурного подразделения объяснительную записку Нарушителя ИБ. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение (двух) рабочих дней и представлена его непосредственным руководителем администратору ИБ в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить объяснительную

записку, ответственный за информационную безопасность составляет акт, составленный в соответствии сустановленным в Учреждении порядке.

4.2.8. Ответственный за информационную безопасность проводит оценку негативных последствий от реализации Инцидента ИБ. В ходе данной оценки учитываются:

прямой финансовый ущерб;

репутационный ущерб;

потенциальный ущерб;

косвенные потери, связанные с недоступностью сервисов, потерей информации;

другие виды ущерба или аспекты негативных последствий для Учреждения или субъектов персональных данных.

4.2.9. С целью минимизации последствий Инцидента ИБ возможно временное отключение прав доступа сотрудника к Информационным ресурсам (ИР) на время проведения расследования. Подобное отключение инициируется ответственным за информационную безопасность с обязательным предварительным устным согласованием с руководителем сотрудника.

4.2.10. В случае, если у Нарушителя ИБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам ответственный за информационную безопасность по согласованию с руководителем Нарушителя ИБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у Нарушителя ИБ прав доступа к ИР либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным Порядком доступа к информационным, программным и аппаратным ресурсам Учреждения. Если Нарушение ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с информационными ресурсами, то основанием для возврата прав доступа является успешное прохождение инструктажа по информационной безопасности, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами Учреждения.

4.2.11. Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИР (разблокировка пользователя) может производиться только ответственным за информационную безопасность.

5. Оформление результатов проведенного разбирательства

5.1. Собранная в процессе разбирательства Инцидента ИБ информация фиксируется ответственным за информационную безопасность в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по Инциденту ИБ *(Приложение №1)*.

5.2. Ответственный за информационную безопасность формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию Инцидента ИБ.

5.3. Итоговое заключение по Инциденту ИБ ответственный за информационную безопасность направляет руководителям структурных подразделений, затронутых Инцидентом ИБ.

5.4. Ответственный за информационную безопасность фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

5.5. Ответственный за информационную безопасность, при необходимости определения правовой оценки Инцидента ИБ, может обратиться за консультациями к юристу Учреждения.

5.6. В случае выявления в Инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, ответственный за информационную безопасность передает все материалы по Инциденту ИБ руководству Учреждения для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

6. Завершение разбирательства, превентивные мероприятия

6.1. По завершению разбирательства Инцидента ИБ, ответственный за информационную безопасность передает имеющиеся материалы (в объеме, достаточном для принятия решения) вышестоящему руководителю Нарушителя ИБ для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

6.2. На основании полученных результатов разбирательства руководитель структурного подразделения совместно с ответственным за информационную безопасность в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у Нарушителя ИБ;
- доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов Учреждения;
- обсуждение Инцидента ИБ на совещании руководителей или собрании коллектива;
- отмена неактуальных прав доступа к информационным ресурсам;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

6.3. О результатах проведенного разбирательства Инцидента ИБ ответственный за информационную безопасность по необходимости инициирует подготовку сообщения об Инциденте ИБ в адрес руководства Учреждения.

7. Права, обязанности и ответственность участников разбирательства

7.1. Ответственный за информационную безопасность имеет право:

- По согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам Инцидента ИБ у Нарушителя ИБ.

- Запрашивать и получать от руководителей и сотрудников Учреждения, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента ИБ.

- Инициировать отключение от информационных ресурсов сотрудников Учреждения, 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.

- По результатам расследования Инцидента ИБ инициировать изменения в бизнес-процессах и информационных ресурсах Учреждения с целью повышения их защищенности и снижения рисков Инцидентов ИБ.

- Инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной и (или) материальной ответственность согласно внутренним нормативным документам Учреждения.

7.2. Ответственный за информационную безопасность 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 Учреждения и начальнику отдела информатизации.

- Проводить анализ обстоятельств, способствовавших совершению каждого Инцидента ИБ, и на его основе, совместно с отделом информационных технологий, разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных Инцидентов ИБ и минимизации возможности их повторения в будущем.

7.3. Руководители структурных подразделений и сотрудники Учреждения обязаны:

- предоставлять по запросам администратора ИБ устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства Инцидента ИБ;

- информировать ответственного за информационную безопасность о выявленных Инцидентах ИБ;

- информировать отдел информатизации об имеющихся запросах и обращениях субъектов персональных данных.

Приложение 1 **к Регламенту**

Карточка данных о инциденте ИБ.

Дата события
Номер события

Информация о сообщающем лице

Фамилия _____ Адрес _____

Организация _____ _____

Телефон _____ Электронная почта _____

Описание события ИБ

Описание события:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на административный (учебный) процесс
- Любые идентифицированные уязвимости

Детали события ИБ

Дата и время возникновения события
Дата и время обнаружения события

Дата и время сообщения о событии
Классификация события
Закончилось ли событие? *(отметить квадрат)* Да ☐ Нет ☐
Если «да», то уточнить, как долго длилось событие в днях/часах/минутах

Тип инцидента ИБ

(Отметить один квадрат, затем заполнить соответствующие поля ниже)

Действительный ☐ **Попытка** ☐ **Подозрение** ☐

(Один из) **Намеренная** ☐ *(указать типы угрозы)*

Хищение ☐
Мошенничество ☐
Саботаж/физический ущерб ☐
Вредоносная программа ☐
Хакерство/Логическое проникновение ☐
Неправильное использование ресурсов ☐
Другой ущерб ☐

Определить:

(Один из) **Случайная** ☐ *(указать типы угрозы)*

Отказ аппаратуры ☐
Отказ ПО ☐
Отказ связи ☐
Пожар, наводнение ☐
Отказ электропитания ☐
Другие природные события ☐

Определить:

Потеря существенных сервисов ☐
Недостаточное кадровое обеспечение ☐
Другие случаи ☐

Определить:

(Один из) **Ошибка** ☐ *(указать типы угрозы)*

Операционная ошибка ☐
Ошибка аппаратной поддержки ☐
Ошибка поддержки ПО ☐
Ошибка пользователя ☐
Ошибка конструкции ☐
Другие случаи (включая истинные заблуждения) ☐

Определить:

Неизвестно ☐

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)

Определить:

Пораженные активы

Пораженные активы (если есть) *(Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности)*

Информация/Данные _____

Аппаратура _____

Программное обеспечение _____

Средства связи _____

Документация _____

Негативное воздействие инцидента на административный (учебный) процесс

Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на бизнес по шкале 1÷10, используя сокращения (указатели категорий): (ФП) – финансовые потери/разрушение бизнес-операций, (КИ) - коммерческие и экономические интересы, (ПД) – информация, содержащая персональные данные, (ПО) – правовые и нормативные обязательства, (БО) – менеджмент и бизнес-операции, (ПП) – потеря престижа Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»

		Значимость	**Указатели**	**Стоимость**
Нарушение конфиденциальности *(т. е., несанкционированное раскрытие)*	☐			
Нарушение целостности *(т. е., несанкционированная модификация)*	☐			
Нарушение доступности *(т. е., недоступность)*	☐			
Нарушение неотказуемости	☐			
Уничтожение	☐			

Полные стоимости восстановления после инцидента

(Где возможно, необходимо указать общие расходы на восстановление после инцидента в целом по шкале 1÷10 для «значимости» и в деньгах для «стоимости»)	**Значимость**	**Указатели**	**Стоимость**

Разрешение инцидента

Дата начала расследования инцидента _____

Фамилия лица (лиц), проводившего (их) расследование инцидента _____

Дата окончания инцидента _____

Дата окончания воздействия _____

Дата завершения расследования инцидента _____

Ссылка и место хранения отчета о расследовании _____

Причастные лица

(Один из)

Лицо ☐

Организованная группа ☐

Легально учрежденная организация/учреждение ☐

Случайность ☐

Нет виновного ☐

Например, природные факторы, отказ оборудования, ошибка человека

Описание нарушителя

Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода ☐

Политика/Терроризм ☐

Развлечение/хакерство ☐

Реванш ☐

Другие мотивы ☐

Определить:

Действия, <u>предпринятые</u> для разрешения инцидента

(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением...»)

Действия, запланированные для разрешения инцидента

(например, см. выше)

Прочие действия

(например, по-прежнему требуется проведение расследования для другого персонала)

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный ☐ **Незначительный** ☐

(Укажите любые другие заключения) _____

Ознакомленные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия

Администратор ИБ ☐
Руководитель подразделения (уточнить какого) ☐
Автор отчета ☐
Полиция ☐
Руководитель организации ☐
Начальник отдела информатизации ☐
Начальник отдела кадров ☐
Другое лица ☐

(например, служба охраны, регулятивного органа, сторонняя организация)
Определить:

Привлеченные лица

Инициатор		Аналитик		Аналитик	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Роль	_____	Роль	_____	Роль	_____
Дата	_____	Дата	_____	Дата	_____