

3.3.2. При наличии нарушений I и II категорий блокирует доступ к ИСПДн работника (работников) Учреждения, действия которых предположительно стали причиной выявленного инцидента.

3.3.3. Принимает необходимые меры по устранению последствий выявленного инцидента, определяет перечень мероприятий по предотвращению в будущем аналогичных инцидентов (далее - профилактические мероприятия), фиксирует их выполнение.

3.3.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (нарушения I категории):

3.3.4.1. Незамедлительно уведомляет директора об инциденте, обо всех обстоятельствах, указанных в подпунктах 3.3.4.2., 3.3.4.3., а также подает служебную записку и проект приказа о проведении расследования. Информация о мерах по устранению последствий инцидента должна быть представлена директору до принятия указанных мер.

3.3.4.2. В течение двадцати четырех часов с момента выявления инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом, в порядке, предусмотренном действующим законодательством и подзаконными нормативными актами. Уведомление осуществляется с использованием функционала официального сайта уполномоченного органа.

3.3.4.3. В течение семидесяти двух часов с даты утверждения результатов расследования выявленного инцидента уведомляет уполномоченный орган по защите прав субъектов персональных данных о результатах расследования, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии). Уведомление осуществляется с использованием функционала официального сайта уполномоченного органа.

3.3.4.4. Руководит расследованием, обеспечивает соблюдение комиссией требований действующего законодательства и иных нормативных правовых актов, а также локальных нормативных актов и организационно-распорядительных документов Учреждения, в том числе приказа о проведении расследования.

3.3.4.5. Обеспечивает надлежащее и своевременное выполнение профилактических мероприятий.

3.4. Регистрация инцидентов информационной безопасности осуществляется в «Журнале по учету мероприятий по контролю обеспечения защиты персональных данных в ИСПДн» (далее - Журнал). Регистрации подлежат инциденты, составляющие нарушение I и II категории.

3.5. Любая информация предоставляется в уполномоченный орган по защите прав субъектов персональных данных (подпункты 3.3.4.2., 3.3.4.3.) после предварительного согласования с директором.

3.6. Профилактические мероприятия определяются:

3.6.1. В отношении нарушений I категории - по результатам расследования, с фиксацией в Журнале содержания мероприятий и результатов их выполнения.

3.6.2. В отношении нарушений II категории - председателем комиссии самостоятельно, с фиксацией в Журнале содержания мероприятий и результатов их выполнения.

3.6.3. В отношении нарушений III категории - председателем комиссии самостоятельно.

3.7. Информацию о выявленных нарушениях II и III категории председатель комиссии представляет директору служебной запиской ежемесячно, в срок не позднее пятого рабочего дня месяца, следующего за отчетным. При отсутствии в отчетном месяце соответствующих нарушений служебная записка не подается.

4. Порядок назначения расследования

4.1. Расследование назначается по нарушениям I категории.

4.2. Расследование назначается приказом директора на основании служебной записки председателя комиссии.

7.1.7. Обеспечение при проведении расследования соблюдения требований действующего законодательства и иных нормативных правовых актов, а также локальных нормативных актов и организационно-распорядительных документов учреждения, в том числе приказа о проведении расследования (пункт 3.3.4.4.).

7.2. Ответственный(ые) за обеспечение безопасности персональных данных несут ответственность за:

7.2.1. Своевременное сообщение об инциденте ответственному за организацию обработки персональных данных, а также председателю комиссии (пункт 3.2.1.).

7.2.2. Надлежащее выполнение указаний председателя комиссии в части мер по устранению последствий выявленного инцидента, а также профилактических мероприятий (пункт 3.2.2.).

7.3. Иные работники Учреждения несут ответственность за:

7.3.1. Принятие мер по установлению достоверности полученной информации об инциденте информационной безопасности (пункт 3.1.1.).

7.3.2. Своевременное сообщение об инциденте информационной безопасности ответственному за обеспечение безопасности персональных данных (пункт 3.1.2.).

7.3.3. Надлежащее выполнение указаний, полученных от ответственного за обеспечение безопасности персональных данных, а также ответственного за организацию обработки персональных данных, и председателя комиссии (пункт 3.1.3.).

Журнал

по учету мероприятий по контролю обеспечения защиты персональных данных в ИСПДн
(форма)

Раздел 1. Мероприятия по контролю обеспечения защиты персональных данных в ИСПДн

Название мероприятия	Дата начала и окончания проверки	Исполнитель/ Проверяющий	Результат проверки	Подпись, ФИО ответственного лица	Примечание
1	2	3	4	5	6

Раздел 2. Инциденты информационной безопасности

Дата регистрации, категория нарушения	Описание инцидента	Предполагаемые причины нарушения прав субъектов ПД	Предполагаемый вред правам субъектов ПД	Принятые меры по устранению последствий	Профилактические мероприятия	Отметка об исполнении мероприятия	Подпись, Ф.И.О. председателя комиссии
1	2	3*	4	5	6	7	8

* Заполняется только для нарушений I категории.