УТВЕРЖДАЮ

Директор ГБОУ СО «Верхнесинячихинская
школа-интернат»

\_\_\_\_\_\_\_\_\_\_\_\_\_ О.А. Бурухина

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

Регламент реагирования на инциденты безопасности персональных данных в информационных системах персональных данных

ГБОУ СО «Верхнесинячихинская школа-интернат»

# Общие положения

Настоящий регламент разработан в соответствии с требованиями Федерального закона № 152-ФЗ от 27.07.2006г. «О персональных данных», приказа Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также прочих нормативных документов по защите информации.

Настоящий Регламент определяет единый и обязательный порядок реагирования на возникшие инциденты информационной безопасности, единый порядок проведения служебных расследований, а также проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов информационной безопасности в информационных системах персональных данных (далее – ИСПДн)
ГБОУ СО «Верхнесинячихинская школа-интернат» (далее – Учреждение).

# Определение инцидента информационной безопасности

К инцидентам информационной безопасности в ИСПДн (далее – инциденты ИБ) относятся:

* нарушение конфиденциальности, целостности или доступности персональных данных (далее – ПДн);
* отказ оборудования, сервисов, средств обработки и (или) защиты ПДн;
* несоблюдение требований внутренней организационно-распорядительной документации и действующего законодательства Российской Федерации в области защиты и обработки персональных данных;
* заражение вредоносными программами информационных систем персональных данных.

К инцидентам информационной безопасности в ИСПДн также относятся попытки и факты получения несанкционированного доступа к информационным системам персональных данных:

* сеансы работы в ИСПДн незарегистрированных пользователей;
* сеансы работы Пользователей ИСПДн с нарушением установленного времени доступа;
* сеансы работы Пользователей ИСПДн, срок действия полномочий которых истек либо в состав полномочий которых не входят выявленные действия с ПДн;
* действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;
* совершение попыток несанкционированного доступа к персональной рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
* несанкционированное внесение изменений в конфигурации программных или аппаратных средств обработки или защиты ПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для наступления случаев, описанных выше.

# Порядок реагирования на инциденты информационной безопасности

## Оповещение об инциденте информационной безопасности

Последовательность действий работника в случае выявления инцидента ИБ:

* прекратить работу с ресурсом, в котором выявлен инцидент ИБ;
* оповестить непосредственного руководителя о факте выявления инцидента ИБ;
* непосредственный руководитель работника должен оповестить ответственного за реагирование на инциденты;
* ответственный за реагирование на инциденты проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его наступлению, и составляет краткую справку, в которой описываются произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ.
* информацию об инциденте необходимо зафиксировать в «Журнале учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств на средствах вычислительной техники в информационных системах персональных данных ГБОУ СО «Верхнесинячихинская школа-интернат».

## Мероприятия при наступлении инцидента информационной безопасности, ставшего причиной негативных последствий для субъекта ПДн

В случае если инцидент ИБ может стать (или уже стал) причиной негативных последствий для субъектов ПДн, персональные данные этих субъектов необходимо немедленно блокировать до устранения причин, повлекших наступление инцидента ИБ и его последствий. Решение о блокировании персональных данных принимает ответственный за организацию обработки и обеспечение безопасности персональных данных. Для этой цели временно прекращается обработка (далее – блокировка) персональных данных субъекта.

Ответственный за организацию обработки и обеспечение безопасности уведомляет субъекта о блокировании его персональных данных.

Персональные данные остаются заблокированными до устранения причин, повлекших наступление инцидента ИБ.

Если причины возникновения инцидента ИБ невозможно устранить, то персональные данные должны быть уничтожены. Ответственный за организацию и обработку и обеспечение безопасности персональных данных обеспечивают немедленное уничтожение персональных данных.

Ответственный за организацию обработки и обеспечение безопасности персональных данных оповещает субъекта персональных данных о прекращении обработки и уничтожении его персональных данных.

## Устранение последствий и причин инцидента информационной безопасности

Обязанности по устранению последствий и причин инцидента информационной безопасности возлагаются на ответственного за реагирование на инциденты. Не позднее трех рабочих дней с момента наступления инцидента ответственный за реагирование на инциденты совместно с ответственным за организацию обработки и обеспечение безопасности персональных данных составляет План устранения последствий и причин наступления инцидента информационной безопасности. В данный план целесообразно включить:

* общую информацию о произошедшем инциденте;
* анализ ситуации, оперативные контрмеры, которые можно применить для локализации инцидента;
* определение лиц, ответственных за расследование и установление причин, по которым стало возможным наступление инцидента;
* определение лиц, ответственных за проведение профилактических мероприятий, разработку и внедрение мер по недопущению повторного наступления инцидента.

## Проведение расследования инцидента информационной безопасности

Разбирательство и составление отчетов в обязательном порядке должны проводиться в случае выявления следующих фактов:

* нарушение конфиденциальности, целостности, доступности персональных данных;
* халатность и несоблюдение требований по обеспечению безопасности персональных данных;
* несоблюдение условий хранения носителей персональных данных;
* использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

Задачами внутреннего расследования являются:

* установление обстоятельств нарушения, в том числе времени, места и способа
* его совершения;
* установление лиц, непосредственно виновных в данном нарушении;
* выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования осуществляется комиссией (далее – Комиссия), назначенной приказом директора Учреждения для проведения расследования.

Комиссия должна приступить к работе по расследованию не позднее следующего дня после даты выявления нарушения.

Общая продолжительность внутреннего расследования не должна превышать одного календарного месяца.

Права и обязанности комиссии:

* опрос работников, допустивших нарушение конфиденциальности информации,
* а также лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;
* проведение осмотров объектов и предметов, которые могут иметь отношение к факту нарушения;
* привлечение (с разрешения соответствующего руководителя) других работников к проведению отдельных действий в рамках внутреннего расследования.

 Работник, в отношении которого проводится расследование, должен быть ознакомлен с приказом руководителя о проведении расследования.

Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (актами, справками и т. п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии (не менее чем за двумя подписями).

В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения директора Учреждения.

Для организованного и оперативного проведения внутреннего расследования ответственный за реагирование на инциденты совместно с ответственным за организацию обработки и обеспечение безопасности персональных данных разрабатывает версии причин и составляет план проведения необходимых мероприятий по каждой из этих версий. В ходе расследования могут выдвигаться и отрабатываться дополнительные версии, в этом случае план действий уточняется.

Одновременно с проведением внутреннего расследования, директор Учреждения может поручить Комиссии определить актуальность утраченных персональных данных, а также определить (подсчитать) ущерб (убытки) по расследуемому факту. В отдельных случаях такая оценка может быть осуществлена специализированной организацией.

По окончании внутреннего расследования Комиссия представляет директору Учреждения отчет, в котором излагаются:

* основания и время проведения расследования;
* проделанная работа (кратко);
* время, место и обстоятельства факта нарушения;
* причины и условия совершения нарушения;
* виновные лица и степень их вины;
* наличие умысла в действиях виновных лиц;
* предложения по возмещению ущерба;
* предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
* рекомендации по исключению подобных нарушений;
* другие вопросы, поставленные перед комиссией (об актуальности персональных данных, о размерах ущерба и т.д.).

К отчету прилагаются:

* письменные объяснения лиц, которых опрашивали члены Комиссии;
* акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т.д.;
* другие документы (копии документов), относящиеся к расследованию, в то числе заключения по определению размеров ущерба (убытков).

Отчет должен быть подписан всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая отчет, приобщает к нему свое особое мнение (в письменном виде).

Отчет по результатам расследования подлежит утверждению директором Учреждения.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель, имеют право знакомиться с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с отчетом по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях лица признаков административного правонарушения или уголовного преступления руководитель обязан обращаться в правоохранительные органы для привлечения виновного к ответственности в соответствии с законодательством Российской Федерации. В соответствии с Трудовым кодексом возмещение ущерба проводится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае отчета по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нарушение режима конфиденциальности.

## Превентивные меры по недопущению возникновения инцидентов информационной безопасности

Для того, чтобы предупредить или максимально уменьшить вероятность наступления инцидента необходимо проводить мероприятия по осуществлению внутреннего контроля соответствия процесса обработки персональных данных требованиям к защите информации в соответствии с «Инструкцией по осуществлению внутреннего контроля соответствия процесса обработки персональных данных требованиям к защите информации в информационных системах персональных данных ГБОУ СО «Верхнесинячихинская школа-интернат».

## Оценка эффективности реализованных мер в рамках системы защиты персональных данных

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится комиссией по проведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных.

Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных Учреждения организуется и проводится ответственным за организацию обработки и обеспечение безопасности персональных данных и администратором безопасности.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер и контроль за выполнением требований защиты персональных данных в информационных системах персональных данных проводится администратором безопасности информационных систем персональных и ответственным за организацию обработки и обеспечение безопасности персональных данных не реже 1 раза в 12 месяцев. Итоги проведенных мероприятий по проверке состояния защиты персональных данных вносятся в План внутренних проверок состояния защиты персональных данных в ИСПДн.

# Ответственность

Ответственность за организацию процесса реагирования на инциденты возлагается на ответственного за реагирование на инциденты.

Контроль за выполнение требований данного регламента возлагается на ответственного за организацию обработки и обеспечение безопасности персональных данных.

Соблюдение требований настоящего регламента возлагается на всех сотрудников, являющихся пользователями ИСПДн.

Нарушение требований настоящего регламента влечет за собой ответственность, предусмотренную законодательством Российской Федерации.

**РАЗРАБОТАНО:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ответственный за организацию обработки и обеспечение безопасности персональных данных |  |  |  | А.Е. Запольских |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

**С документом ознакомлен (а):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Директор  |  |  |  | О.А. Бурухина  |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Администратор безопасности ИСПДн  |  |  |  |  | Н.А. Блохин |
|  |  |  | (подпись, дата) |  | (инициалы, фамилия) |

Приложение №1

**Лист ознакомления с регламентом**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Ф.И.О.****работника** | **Личная подпись** | **Дата ознакомления** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |