Приложение 17

УТВЕРЖДЕН
распоряжением
администрации
от 23.07.2021 *№* 82

ПОРЯДОК

реагирования на инциденты информационной безопасности в администрации муниципального образования «Бугровско сельское поселение» Всеволожского муниципального района Ленинградской области

п.Бугры
2021 г.

1. Термины и определения

В настоящем Порядке использованы следующие термины и определения:

Безопасность персональных данных: Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных: Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вредоносное программное обеспечение: Программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации: Возможность получения информации и ее использования.

Защита информации: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Идентификация: Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных: Информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таковых средств.

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

Использование персональных данных: Действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом, затрагивающих права и свободы субъекта ПДн или других лиц.

Конфиденциальность персональных данных: Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия): Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

Обработка персональных данных: Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение

(обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Персональные данные: Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн) в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь персональных данных: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

Процесс обработки персональных данных: Процесс, в котором присутствует обработка персональных данных.

Средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Уничтожение персональных данных: Действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

Целостность информации: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Доступность информации - Свойство информационной безопасности, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

2. Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

№ п/п	Сокращение	Описание
1.	**ИБ**	Информационная безопасность
2.	**ИСПДн**	Информационная система ПДн
3.	**НСД**	Несанкционированный доступ
4.	**ПДн**	Персональные данные

3. Область применения

Настоящий Порядок реагирования на инциденты информационной безопасности (далее - Порядок) предназначен для определения единого порядка реагирования на возникшие инциденты информационной безопасности, проведения служебных расследований, а также проведения мероприятий,

нацеленных на предотвращение наступления повторных инцидентов в администрации МО «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области (далее по тексту - администрация).

Требования настоящего Порядка распространяются на должностных лиц администрации, отвечающие за обеспечение безопасности ПДн.

4. Общие положения

Настоящий Порядок разработан в соответствии с Политикой администрации в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-фз «О персональных данных».

В соответствии с настоящим Порядком к инцидентам ИБ в администрации относятся:

- нарушение конфиденциальности, целостности или доступности ПДн;
- отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;
- несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);
- заражение программных компонентов ИСПДн вредоносным программным обеспечением.

К инцидентам ИБ в ИСПДн также относятся попытки и факты получения НСД к ИСПДн:

- сеансы работы в ИСПДн незарегистрированных пользователей;
- 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 выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.
- совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
- несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки, или защиты, входящих в состав ИСПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для возникновения описанных выше инцидентов.

5. Оповещение об инциденте информационной безопасности

В случае выявления инцидента ИБ устанавливается следующая последовательность действий сотрудников администрации:

1) прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

2) оповестить своего непосредственного руководителя о факте выявления инцидента ИБ;

3) руководитель должен оповестить должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн;

4) после извещения указанных должностных лиц по их требованию предоставить всю необходимую информацию.

Должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ. Справка направляется главе администрации для принятия решения о проведении расследования инцидента ИБ.

Порядок проведения расследования инцидента ИБ описан в разделе 7 настоящего документа.

Мероприятия по устранению причин и недопущению повторного возникновения инцидента ИБ описаны в разделе 8 настоящего документа.

6. Мероприятия при возникновении инцидента информационной безопасности, ставшего причиной возникновения негативных последствий для субъекта ПДн

В случае если инцидент ИБ может стать (или уже стал) причиной возникновения негативных последствий для субъектов ПДн, необходимо немедленно блокировать ПДн этих субъектов до устранения причин, повлекших за собой возникновение инцидента ИБ. Решение о блокировании ПДн принимает должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн.

ПДн остаются заблокированными до устранения причин, повлекших за собой возникновение инцидента ИБ.

7. Проведение расследования инцидента информационной безопасности

Внутреннее расследование и составление заключений должно в обязательном порядке проводиться в случае выявления:

- нарушения конфиденциальности, целостности или доступности ПДн;
- халатности и несоблюдения требований по обеспечению безопасности ПДн;
- несоблюдения условий хранения носителей ПДн;

- использования СЗИ, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

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 проводится по решению главы администрации. С целью проведения расследования в обязательном порядке формируется Комиссия, в состав которой входят должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн и системный администратор, юрист и иные должностные лица администрации, участие которых может потребоваться.

Комиссия должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать одного месяца.

В рамках проведения расследования инцидента ИБ Комиссия уполномочена:

- проводить опрос сотрудников администрации, по вине которых предположительно произошел инцидент ИБ, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;
- проводить осмотр объектов и предметов, которые могут иметь отношение к инциденту ИБ;

По решению главы администрации на Комиссию могут быть возложены дополнительные обязанности и права.

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

Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки 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 в виде протокола.

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

Для оперативного проведения внутреннего расследования должностное лицо ответственного за защиту ПДн составляет План проведения расследования.

Одновременно с проведением внутреннего расследования, глава администрации может поручить Комиссии определить ущерб для администрации и (или) для субъекта ПДн от произошедшего инцидента ИБ. В отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

По окончании внутреннего расследования Комиссия представляет главе администрации отчет по результатам расследования, 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 конфиденциальной информации, 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 том числе заключения по определению размеров ущерба.

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

Отчет подлежит утверждению главой администрации.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления 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 распоряжением.

При наличии в действиях работника распоряжений административного правонарушения или уголовного преступления глава администрации обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с положениями нормативных документов РФ.

В соответствии с Трудовым кодексом РФ, возмещение ущерба производится 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 заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

Первый экземпляр отчета с резолюцией главы администрации, копия распоряжения (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дела о внутренних расследованиях хранятся у главы администрации.

8. Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение, в зависимости от произошедшего инцидента ИБ, включают в себя:

- мониторинг событий в информационной системе ПДн;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе ПДн;
- контроль действий системных администраторов;
- проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности ПДн;
- ознакомление пользователей с мерами ответственности, установленными нормативными документами РФ, за нарушение норм и правил обработки ПДн, а также за разглашение полученных данных.

9. Пересмотр и внесение изменений

Настоящий Порядок должен пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;
- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;

Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн в администрации.

Внесение изменений производится на основании соответствующего распоряжения администрации.