УТВЕРЖДАЮ

Ректор Автономной некоммерческой организации высшего образования «Институт непрерывного образования»

_____ Л.С. Цветлюк

«__» _____ 2017г.

Подписано цифровой подписью: АНО ВО "ИНО"
DN: ОГРН=1087746806311, STREET=Шоссе Энтузиастов д. 56 стр.32 офис 214, ИНН=007720623379, C=RU, L=г. Москва, S=77 г. Москва, E=ca@astralm.ru, O="ООО ""АСТРАЛ-М""", CN="ООО ""АСТРАЛ-М"""
Причина: Я утвердил этот документ
Местонахождение: г. Москва, Рязанский пр-т, 86/1
Дата: 30 Декабрь 2020 г. 12:49:38

РЕГЛАМЕНТ ПО ПРОВЕДЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ И РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Москва, 2017 г.

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных– обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных– передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Типовая информационная система– информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

Специальная информационная система– информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

2. ОБЩИЕ ПОЛОЖЕНИЯ

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. Так же настоящий документ устанавливает правила обновления локальной документации в области персональных данных в Автономной некоммерческой организации высшего образования «Институт непрерывного образования» (далее – Оператор).

3. ОПРЕДЕЛЕНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИСПДн

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

- нарушение конфиденциальности, целостности или доступности 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 и 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.

4. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 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 Администратора безопасности ИСПДн о факте выявления инцидента;

– после извещения ответственных сотрудников по их решению представить всю необходимую информацию.

Администратор безопасности ИСПДн 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.

4.2 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 Администратор безопасности ИСПДн. Для этой цели Администратор безопасности ИСПДн блокирует персональные данные.

Ответственный за организацию обработки ПДн 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 обработки ПДн и Администратор безопасности ИСПДн обеспечивают немедленное уничтожение персональных данных.

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

4.3 Устранение последствий и причин инцидента информационной безопасности

Обязанности по устранению последствий и причин инцидента информационной безопасности возлагаются на Администратора безопасности ИСПДн. Не позднее трех дней с момента наступления инцидента Администратор безопасности ИСПДн 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.

4.4 Проведение расследования инцидента информационной безопасности

Разбирательство и составление заключений 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 возлагается приказом руководителя на Комиссию по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Комиссия). Комиссия должна приступить к работе по расследованию не позднее следующего дня после даты выявления нарушения.

Общая продолжительность внутреннего расследования не должна превышать одного 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 руководителя Оператора.

Для организованного и оперативного проведения внутреннего расследования Администратор безопасности ИСПДн 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, руководитель Оператора может поручить Комиссии определить актуальность утраченной (разглашенной) конфиденциальной информации, 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 руководителю Оператора заключение, 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 заключению 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 (убытков).

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

Заключение по результатам расследования подлежит утверждению руководителя Оператора.

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 заключением 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 заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нарушение режима конфиденциальности.

Первый экземпляр заключения с резолюцией руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дело о внутренних расследованиях вносится в номенклатуру дел Оператора.

4.5 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 персональных данных;
- восстановление операционной системы рабочей станции, на которой произошел инцидент ИБ, на заводские настройки;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе персональных данных;
- контроль над действиями системных администраторов;
- проведение обучения (повторного обучения) пользователей правилам обработки и защиты персональных данных;

– ознакомление пользователей с мерами ответственности, установленными законодательством Российской Федерации за нарушение норм и правил обработки персональных данных, а также за разглашение полученных данных;

– пересмотр организационно-распорядительной документации, устанавливающей правила обработки и обеспечения безопасности при работе с персональными данными.

5. 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 Оператора организуется и проводится администратором безопасности информационных систем персональных данных.

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 ПДн 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 (Приложение 1).

6. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ДОКУМЕНТЫ ОПЕРАТОРА

Пересмотр положений настоящего и иных локальных документов Оператора, касающихся вопросов обработки и обеспечения безопасности персональных данных, проводится в следующих случаях, если иное не установлено в пересматриваемых документах:

- на регулярной основе, но не реже одного раза в полгода;
- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;
- по результатам внутреннего контроля (аудита) системы защиты персональных данных в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности персональных данных и выявивших недостатки в правилах предоставления доступа к персональным данным.

Ответственным за пересмотр настоящего Регламента является Администратор безопасности ИСПДн и Ответственный за организацию обработки ПДн.

Внесение изменений производится на основании соответствующего приказа руководителя Оператора.

Приложение 1

План внутренних проверок

состояния защиты персональных данных в ИСПДн

Наименование мероприятий	**Срок/периодичность**	**Ответственный/исполнитель**
Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных	1 раз в 12 месяцев	Ответственный за организацию обработки ПДн
Оценка эффективности реализованных в рамках системы защиты персональных данных мер	1 раз в 12 месяцев	Администратор безопасности ИСПДн