ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
INSTITUTE OF PROFESSIONAL EDUCATION

115114, г. Москва, Дербеневская набережная, д. 11 Тел.: (495) 120-79-01

Научная автономная некоммерческая организация «Институт профессионального образования»
Р/с 40703810338000016474 в ПАО СБЕРБАНК, к/с 30101810400000000225, БИК 044525225
ИНН 9725024950 КПП 772501001 ОКАТО 45296559000 ОКПО 42319365 ОКВЭД 72.20 ОГРН 1197700016623

ПРИКАЗ

г. Москва

«29» декабря 2022 г. № 2-ПД

Об утверждении Плана мероприятий по обеспечению Безопасности персональных данных, Перечня мероприятий по защите персональных данных – утверждении Положения о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных в Научной автономной некоммерческой организации «Институт профессионального образования» (далее- НАНО «ИПО»)

В целях исполнения требований Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 21 марта 2012 года № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", **приказываю:**

1. Утвердить Перечень мероприятий по защите персональных данных НАНО «ИПО».
2. Утвердить Положение о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных.
3. Ректору – Бородиной М.И., обеспечить размещение настоящего приказа и утвержденных Положений на сайте НАНО «ИПО».
4. Контроль исполнения Приказа возложить на Ректора – Бородину М.И.

Приложение:

1. Перечень мероприятий по защите персональных данных НАНО «ИПО».
2. Положение о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных.

Ректор
НАНО «ИПО» Бородина М.И.

М.П.

Приложение
к приказу НАНО «ИПО»
от «29» декабря 2022 г. № 2-ПД

План
Мероприятий по обеспечению безопасности персональных данных

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее - План мероприятий) содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в НАНО «ИПО».

План мероприятий составлен на основании списка мер, методов и средств защиты, определенных в Политике в отношении обработки персональных данных.

Выбор конкретных мероприятий осуществляется на основании анализа Отчета о результатах обследования ИСПДн и Модели угроз безопасности.

В План мероприятий включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План мероприятий включена следующая информация:

- название мероприятия;
- исполнитель мероприятия/ответственный за исполнение;
- итог выполнения мероприятия.

Меры (мероприятия) по защите персональных данных

Любое юридическое лицо в силу требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обязано принимать меры по защите персональных данных, при этом перечень таких мер оно вправе определять самостоятельно.

Мероприятия по защите персональных данных можно разделить на две большие подгруппы: по внутренней и внешней защите персональных данных.

К мерам по внутренней защите персональных данных относятся следующие действия:

- ограничение числа работников (с регламентацией их должностей), которым открыт доступ к персональным данным. Кого может включать этот перечень? Абсолютно всех, кто имеет доступ к личным делам, т.е. сотрудников отделов кадров или ответственных за кадровое делопроизводство, работников бухгалтерии, секретарей-делопроизводителей, специалистов, которые заключают договоры с физическими лицами, а также инженеров, программистов, юристов;
- назначение ответственного лица, обеспечивающего исполнение организацией законодательства в рассматриваемой сфере;
- утверждение перечня документов, содержащих персональные данные;
- издание внутренних документов по защите персональных данных, осуществление контроля за их соблюдением;
- ознакомление работников действующими нормативами в области защиты персональных данных и локальными актами; проведение систематических проверок соответствующих знаний работников, обрабатывающих персональные данные, и соблюдения ими требований нормативных документов по защите конфиденциальных сведений. Следует иметь в виду, что все сотрудники, которые имеют доступ к персональным данным других людей, должны быть ознакомлены с особенностями законодательства в области защиты персональных данных;
- рациональное размещение рабочих мест для исключения несанкционированного использования защищаемой информации;
- утверждение списка лиц, имеющих право доступа в помещения, в которых хранятся персональные данные;
- утверждение порядка уничтожения информации;

- выявление и устранение нарушений требований по защите персональных данных;

- проведение профилактической работы с сотрудниками по предупреждению разглашения ими персональных данных.

Меры (мероприятия) по внешней защите персональных данных:

- введение пропускного режима, порядка приема и учета посетителей;

- внедрение технических средств охраны, программных средств защиты информации на электронных носителях и др.

Несмотря на то, что законом не установлены конкретные требования к количеству и содержанию локальных актов, принимаемых в организации по вопросам обработки и защиты персональных данных, практика реализации данного нормативного акта сформировала необходимый минимум документов, которые должны быть разработаны в учреждении:

- общий документ, определяющий политику организации в отношении обработки персональных данных, например Политика обработки в отношении персональных данных;

- список лиц, обрабатывающих персональные данные;

- приказ о назначении сотрудника, ответственного за организацию обработки персональных данных. Указанное лицо должно осуществлять внутренний контроль за соблюдением организацией и ее работниками законодательства о персональных данных, в том числе требований к их защите, доводить до сведения персонала положения законодательства о персональных данных, локальных актов по вопросам их обработки, а также требования к защите таких данных, организовывать прием и обработку обращений и запросов субъектов персональных данных и (или) контролировать прием и обработку таких обращений и запросов;

- положение о правовых, организационных и технических мерах защиты персональных данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных. В данном положении прописаны конкретные меры по защите персональных данных (введение пропускного режима, применение программных средств защиты информации - паролей, антивирусных программ, хранение персональных данных обособленно от других сведений, на отдельных материальных носителях и в специально оборудованных помещениях с ограниченным доступом и т. д.);

- локальный акт, устанавливающий процедуры, направленные на предотвращение и выявление нарушений законодательства в сфере защиты персональных данных, устранение последствий таких нарушений. Так, в компании могут быть разработаны план мероприятий по внутреннему контролю безопасности персональных данных, инструкция о порядке проведения служебного расследования по фактам нарушений законодательства в сфере защиты персональных данных, вестись журнал антивирусных проверок и контроля работы с персональными данными, журнал обучения, инструктажа и аттестации по вопросам защиты персональных данных.

2. План мероприятий по обеспечению безопасности ПДн (организационные меры)

№ п/п	Мероприятие	Исполнитель	Итог выполнения мероприятия
1	Утвердить и ознакомить под роспись работников с разработанными организационно-распорядительными документами.	Ответственный за организацию Обработки персональных данных	Выполнение требований ФЗ-152, Постановление Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", требований Постановление Правительства РФ № 1119
2	Добавить пункт о соблюдении конфиденциальности в трудовые договора. Заключить дополнительные соглашения с физическими лицами, в части соблюдения конфиденциальности и обеспечения безопасности персональных данных по приведенному в документах примеру.		Приведение договоров с третьими лицами в соответствие с требования ФЗ
3	При необходимости, заключить дополнительные соглашения с организациями, имеющие доступ к БД ИСПДн - в части соблюдения конфиденциальности и обеспечения безопасности персональных данных по приведенному в документах примеру		Приведение договоров с третьими лицами в соответствие с требования ФЗ-152
4	Получить согласия на, обработку персональных данных сотрудников. Добавить пункт о согласии на обработку ПДн для сбора данных через сайт (Отдельные документы)		Выполнение требований ФЗ-152
5	Оформить с работниками, осуществляющими обработку персональных данных по форме Приложения Приказа «Об организации мероприятий по защите персональных данных» обязательствам неразглашении персональных данных		Выполнение требований ФЗ-152
6	Копию «Политики в отношении обработки персональных» разместить на официальном сайте, в приемной в общедоступном месте.		Выполнение требований ФЗ-152
7	Организовать рассмотрение запросов субъектов ПДн и их		Выполнение требований ФЗ-152

	законных представителей в соответствие с Приложением Приказа «Об организации мероприятий по защите персональных данных»		
8	По номенклатуре дел определить документы, у которых истек срок хранения, уничтожить их' составив Акт об уничтожении - Приложение Типовая форма акта об уничтожении ПДн Приказа «Об организации мероприятий по защите персональных данных»		Приведение в соответствие с требования ФЗ-152 Акты уничтожение носителей ПДн Выполнение требований Постановление Правительства РФ № 687
9	Создать комиссию и утвердить «Акт определения уровня защищенности персональных данных при их обработке в информационной системе»	Оператор ПДн	Выполнение требований 1111 РФ № 1119; Акты определения уровня защищенности персональных данных при их обработке в информационной системе
10	Подписать и направить нарочно или почтовым отправлением Уведомление (изменение в уведомление) об обработке персональных данных в территориальный орган Роскомнадзора	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152
11	При заключении договоров с третьими лицами, оказание услуг которыми подразумевает передачу персональных данных работников, необходимо перед заключением договора получить согласие на передачу персональных данных от сотрудников	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152
12	При заключении договоров с третьими лицами, оказание услуг которыми подразумевает передачу персональных данных работников или доступ третьих лиц к информационной. системе персональных данных необходимо в договор включить соответствующий пункт о	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152
13	Приобретение средств защиты информации (СЗИ) в соответствии с разработанной документацией, технических средств обеспечения ограничения доступа к ИСПДн и местам хранения ПДн	Ответственный за организацию обработки персональных данных	Выполнение требований 1111 РФ № 1119, Приказов ФСТЭК России № 17,21; Отметки в журнале учета СЗИ, СКЗИ
14	Внедрение СЗИ в соответствии с требованиями нормативных актов	Лицензиат ФСТЭК и ФСБ	Выполнение требований 1111 РФ № 1119, Приказа ФСТЭК России № 17,21; Акт установки и ввода в эксплуатацию СЗИ; Эксплуатационная документация на применяемые средства защиты информации

ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
INSTITUTE OF PROFESSIONAL EDUCATION

115114, г. Москва, Дербеневская набережная, д. 11 Тел.: (495) 120-79-01

Научная автономная некоммерческая организация «Институт профессионального образования»
Р/с 40703810338000016474 в ПАО СБЕРБАНК, к/с 30101810400000000225, БИК 044525225
ИНН 9725024950 КПП 772501001 ОКАТО 45296559000 ОКПО 42319365 ОКВЭД 72.20 ОГРН 1197700016623

УТВЕРЖДАЮ:
Ректор НАНО «ИПО»

М.И. Бородина
«29» декабря 2022 г.

ПОЛОЖЕНИЕ
О ПОРЯДКЕ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ
СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В
НАУЧНОЙ АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ «ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»
(Далее- НАНО «ИПО»)

Москва 2022 г.

1. Общие положения

1.1 Настоящее Положение о порядке реагирования на инциденты информационной безопасности (далее - Положение) устанавливает порядок действий лиц, ответственных за обеспечение информационной безопасности при выявлении инцидента информационной безопасности в целях снижения его негативных последствий, а также порядок проведения расследования инцидента информационной безопасности (далее - инцидент).

1.2 Настоящее положение разработано с учетом ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

1.3 Настоящее положение обязательно к исполнению сотрудниками НАНО «ИПО», участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4 В НАНО «ИПО» приказом ректора назначается лицо, ответственное за информационную безопасность - администратор информационной безопасности.

1.5 Разбирательство по всем инцидентам ИБ проводится администратором информационной безопасности с привлечением в необходимых случаях руководителей и работников структурных подразделений.

2. Основные понятия

2.1.В Положении используются следующие понятия и определения:

- ***Информационная безопасность*** - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

- ***Событие информационной безопасности*** - идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности;

- ***Инцидент информационной безопасности*** - появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ;

- ***Обработка инцидентов ИБ*** - деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий;

- ***Закрытие инцидента ИБ*** - действия сотрудников НАНО «ИПО» в рамках реагирования на инцидент ИБ, результатом которых являются:

- устранение нарушений, реализованных в результате Инцидента ИБ;

- устранение причин выявленного Инцидента ИБ;

- выяснение причин нетипичного поведения сотрудников НАНО «ИПО» и (или) иных лиц, нештатного функционирования информационных систем и иных объектов среды информационных активов НАНО «ИПО», а также нетипичных событий в осуществлении технологических процессов.

- ***Персональные данные*** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- ***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;

- ***Информационная система персональных данных*** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Сокращения

3.1. В Положении используются следующие сокращения:

- ИСПДн - информационная система персональных данных;
- ОС - операционная система;
- ПДн - персональные данные;
- СЗИ - средство защиты информации;

- СЗПДн - система защиты персональных данных.

Основными целями обработки Инцидентов ИБ являются:

- создание условий для осуществления своевременного обнаружения и оперативного реагирования на Инциденты ИБГ в том числе их закрытия;

- предотвращение и (или) снижение негативного влияния Инцидентов ИБ на осуществление технологических процессов НАНО «ИПО»; оперативное совершенствование системы обеспечения информационной безопасности НАНО «ИПО».

3.2. Основными задачами обработки Инцидентов ИБ являются:

- своевременное обнаружение инцидентов 1ГБ;

- оперативное реагирование на инциденты ИБ;

- координация деятельности работников структурных подразделений НАНО «ИПО» в рамках процессов реагирования на инциденты ИБ, в том числе их закрытия;

- ведение базы данных зарегистрированных инцидентов ИБ;

- накопление и повторное использование знаний по обнаружению инцидентов 1ГБ и реагированию на них;

- анализ инцидентов ИБ;

- оценка эффективности и совершенствование процессов обработки инцидентов ИБ;

- предоставление руководству информации и отчётов по результатам обработки инцидентов ИБ, в том числе информации о фактах обнаружения инцидентов ИБ и результатах реагирования на них.

4. Обнаружение инцидентов ИБ

4.1. Обнаружение инцидентов 1ГБ выполняется сотрудниками НАНО «ИПО», в том числе с использованием соответствующих технических средств.

4.2. Регистрация информации об инцидентах ИБ, включая сбор информации, выполняется в соответствии с внутренними локальными нормативными документами.

4.3. Основными источниками информации об инцидентах ИБ, связанных с нарушениями требований к обеспечению защиты информации в информационных системах персональных данных, могут быть:

- сообщения сотрудников НАНО «ИПО»;

- сведения, отражённые в журналах регистрации событий информационных систем;

- результаты работы средств защиты информации;

- результаты внутренних проверок;

- другие источники информации об Инцидентах ИБ.

5. Порядок анализа и реагирования на инциденты ИБ

5.1. Администратор ИБ при выявлении инцидентов ИБ реализует комплекс мер, направленных на устранение последствий, причин, вызвавших инцидент, и на недопущение его повторного возникновения.

5.2. Анализ инцидентов ИБ выполняется на основе:

- результатов проведения контроля выполнения процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;

- анализа отчетности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ;

- анализа записей об инцидентах ИБ, содержащих информацию о событиях ИБ, затронутых инцидентом ИБ информационных активах, автоматизированных системах, степени тяжести последствий от обнаруженных инцидентов ИБ.

5.3. В процессе анализа устанавливаются причины возникновения выявленных инцидентов ИБ.

5.4. В процессе анализа определяются наиболее проблемные с точки зрения подверженности инцидентам ИБ сегменты и компоненты информационной инфраструктуры, наиболее существенные уязвимости и недостатки в обеспечении ИБ.

5.5. В процессе анализа инцидентов ИБ оценивается достаточность принятых мер и выделенных ресурсов для реагирования на инциденты ИБ, проводится оценка результатов реагирования на выявленные инциденты ИБ.

5.6. В процессе анализа проверяются действия работников, осуществляемые при реагировании на инциденты ИБ. Целью проведения данной проверки является формирование (инициирование) совершенствований в части:

- корректировки внутренних документов, определяющих порядок обнаружения и реагирования на инциденты ИБ;

- изменения состава лиц, привлекаемых к реагированию на инциденты ИБ;

- корректировки порядка эксплуатации технических средств защиты информации.

5.7. По результатам анализа инцидентов ИБ администратор ИБ формирует акты по результатам обработки инцидентов ИБ (форма акта - приложение 1, форма журнала регистрации - приложение 2).

6. Ответственность

6.1. Все работники, осуществляющие защиту ПДн, обрабатываемых в ИСПДн, обязаны ознакомиться с данным Положением под подпись.

6.2. Сотрудники несут персональную ответственность за выполнение требований настоящего Положения.

7. Срок действия и порядок внесения изменений

7.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым Положением.

7.2. Настоящее Положение подлежит пересмотру не реже одного раза в три года.

Приложение № 1 к Положению о порядке
реагирования на инциденты информационной
безопасности в информационных
системах персональных данных

АКТ *(номер вносится в журнал)*
Об инциденте информационной безопасности
г. Москва

«__» _____ 20___ г. № _____

Инцидент зафиксирован: _____
(дата, фамилия и инициалы работника (-ов))

В инциденте задействованы следующие работники: _____
(дата, фамилия и инициалы работника (-ов))

Описание инцидента: _____

Причины инцидента: _____

Меры, принятые для устранения причин, последствий инцидента:

«___»_____20___г. _____/_____/
(подпись) *(Фамилия И.О.)*

Приложение № 2 к Положению о порядке
реагирования на инциденты информационной
безопасности в информационных
системах персональных данных

ФОРМА ЖУРНАЛА
учета инцидентов информационной безопасности

на	листах	
Начат		20
Окончен		20

Ответственный за ведение журнала:

_____
(ФИО, подпись)

№. п/п	**Краткое описание инцидента**	**Фамилия, имя, отчество, должность сотрудника, обнаружившего инцидент, дата и время обнаружения**	**Дата и время пресечения несанкционированного воздействия**	**Дата, время доведения информации об инциденте в департамент; фамилия, имя, отчество, должность сотрудника, принявшего информацию**	**Подпись системного администратора / администратора безопасности**
1	2	3	4	5	6

Приложение № 2
к Порядку уничтожения и
обезличивания персональных данных

АКТ
уничтожения персональных данных,
обрабатываемых без использования средств автоматизации
г. Москва

«__» _____ 20___г. № ____

Комиссия по уничтожению персональных данных, созданная на основании Приказа Ректора НАНО «ИПО» от «____» _____ 20__г. № 3-ПД, составила акт о том, что ____ _____ 20___г. уничтожила нижеперечисленные носители, содержащие персональные данные, а именно:

Наименование материального носителя, количество листов	**Категории уничтоженных персональных данных**	**Информация о лицах, чьи данные уничтожили**	**Способ уничтожения**	**Причина уничтожения**

Всего _____
(цифрами и прописью)

Настоящий акт составили:
Председатель комиссии: Ильин А.А. /_____/_____/
(ФИО) (подпись) (дата)
Члены комиссии: Акматалиева А. /_____/_____/
(ФИО) (подпись) (дата)
Арбузова А.А. /_____/_____/
(ФИО) (подпись) (дата)

Приложение № 3
к Порядку уничтожения и
обезличивания персональных данных

АКТ

Об уничтожении персональных данных, обрабатываемых с использованием средств автоматизации

г. Москва

«__» _____ 20___ г. № _____

Комиссия по уничтожению персональных данных, созданная на основании Приказа Ректора НАНО «ИПО» от «___» _____ 20___г. № 3-ПД, составила акт о том, что __ __20__ г. уничтожила персональные данные, а именно:

Наименование ИСПДн	**Наименование документа**	**Категория уничтоженных персональных данных**	**Информация о лицах чьи данные уничтожили**	**Способ уничтожения**	**Причина уничтожения**

Всего электронных носителей _____

(цифрами и прописью)

Настоящий акт составили:

Председатель комиссии: Ильин А.А. /_____/_____/

(ФИО) (подпись) (дата)

Члены комиссии: Акматалиева А. /_____/_____/

(ФИО) (подпись) (дата)

Арбузова А.А./_____/_____/

(ФИО) (подпись) (дата)

Приложение № 4
к Порядку уничтожения и
обезличивания персональных данных

Форма выгрузки из журнала регистрации событий и информационной системе персональных данных

Наименование ИСПДн				
Дата	Событие (уничтожение персональных данных)	Категории уничтоженных персональных данных	Информация о лицах, чьи данные уничтожили	Причина уничтожения

*Если ИСПДн не позволяет отобразить причину уничтожения, ответственный за уничтожение указывает ее вручную

Лист ознакомления с Порядком уничтожения и обезличивания персональных данных в НАНО «ИПО»

№ п/п	ФИО	Должность	Дата ознакомления	Подпись