АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«НАУЧНЫЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ»
ИНН 9727127937 КПП 772701001 ОГРН 1267700092296
117218, г. Москва, МО Котловка, ул. Кржижановского, д. 29, к. 5, пом. 8Д/2/4

ПРИКАЗ №30/ОД

г. Москва «02» июня 2026г.

Об утверждении Плана мероприятий по обеспечению безопасности персональных данных, Перечня мероприятий по защите персональных данных и Положения о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных

В целях исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 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»,

ПРИКАЗЫВАЮ:

1. Утвердить План мероприятий по обеспечению безопасности персональных данных в АНО ДПО «Научный институт профессиональных компетенций» (далее – План мероприятий) согласно Приложению № 1 к настоящему приказу.
2. Утвердить Положение о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных в АНО ДПО «Научный институт профессиональных компетенций» (далее – Положение о реагировании) согласно Приложению № 2 к настоящему приказу.
3. Проректору Молокову Н.В.:
   - обеспечить размещение настоящего приказа, Плана мероприятий и Положения о реагировании на официальном сайте Института
   - довести утверждённые документы до сведения всех работников, имеющих доступ к персональным данным, под подпись.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор
АНО ДПО «Научный институт профессиональных компетенций» **Э.М. Панфилова**

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«НАУЧНЫЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ»
ИНН 9727127937 КПП 772701001 ОГРН 1267700092296
117218, г. Москва, МО Котловка, ул. Кржижановского, д. 29, к. 5, пом. 8Д/2/4

Приложение № 1
к приказу ректора
АНО «ДПО «Научный институт
профессиональных компетенций»
от «02» июня 2026 г. № 30/ОД

ПОЛОЖЕНИЕ О ПОРЯДКЕ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В АНО ДПО «НАУЧНЫЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ»

г. Москва, 2026 год

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 (далее – инцидент) в целях снижения его негативных последствий, а также порядок проведения расследования инцидента.

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

1.3. Положение обязательно для исполнения сотрудниками АНО ДПО «Научный институт профессиональных компетенций» (далее – Институт), участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4. В Институте приказом ректора назначается лицо, ответственное за информационную безопасность – администратор информационной безопасности.

1.5. Разбирательство по всем инцидентам 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 защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность;
- **событие информационной безопасности** – идентифицированное появление определённого состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности 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 информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности;
- **обработка инцидентов** – деятельность по своевременному обнаружению инцидентов, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий;
- **закрытие инцидента** – действия сотрудников Института в рамках реагирования на инцидент, результатом которых являются устранение нарушений, устранение причин инцидента, выяснение причин нетипичного поведения сотрудников и (или) иных лиц, нештатного функционирования информационных систем;
- **персональные данные** – любая информация, относящаяся к прямо или косвенно определённому 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;
- **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.

4. Цели и задачи обработки инцидентов информационной безопасности

4.1. Основными целями обработки инцидентов являются:

- создание условий для осуществления своевременного обнаружения и оперативного реагирования на инциденты, в том числе их закрытия;
- предотвращение и (или) снижение негативного влияния инцидентов на осуществление технологических процессов Института;
- оперативное совершенствование системы обеспечения информационной безопасности Института.

4.2. Основными задачами обработки инцидентов являются:

- своевременное обнаружение инцидентов;
- оперативное реагирование на инциденты;
- координация деятельности работников структурных подразделений Института в рамках процессов реагирования на инциденты, в том числе их закрытия;
- ведение базы данных зарегистрированных инцидентов;
- накопление и повторное использование знаний по обнаружению инцидентов и реагированию на них;
- анализ инцидентов;
- оценка эффективности и совершенствование процессов обработки инцидентов;
- предоставление руководству информации и отчётов по результатам обработки инцидентов.

5. Обнаружение инцидентов информационной безопасности

5.1. Обнаружение инцидентов выполняется сотрудниками Института, в том числе с использованием соответствующих технических средств.

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

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

- сообщения сотрудников Института;
- сведения, отражённые в журналах регистрации событий информационных систем;
- результаты работы средств защиты информации;
- результаты внутренних проверок;
- другие источники информации об инцидентах.

6. Порядок анализа и реагирования на инциденты информационной безопасности

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

6.2. Анализ инцидентов выполняется на основе:

- результатов проведения контроля выполнения процессов обнаружения инцидентов и реагирования на них;
- анализа отчётности по обнаружению и реагированию на инциденты;
- анализа записей об инцидентах, содержащих информацию о событиях, затронутых инцидентом информационных активах, автоматизированных системах, степени тяжести последствий.

6.3. В процессе анализа устанавливаются причины возникновения выявленных инцидентов.

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

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

6.6. В процессе анализа проверяются действия работников, осуществляемые при реагировании на инциденты, с целью формирования (инициирования) совершенствований.
6.7. По результатам анализа инцидентов администратор информационной безопасности формирует акты по результатам обработки инцидентов (форма акта – приложение к настоящему Положению) и ведёт журнал регистрации инцидентов (форма журнала – приложение к настоящему Положению).

7. Ответственность

7.1. Все работники, осуществляющие защиту персональных данных, обрабатываемых в ИСПДн, обязаны ознакомиться с данным Положением под подпись.
7.2. Сотрудники несут персональную ответственность за выполнение требований настоящего Положения.

8. Срок действия и порядок внесения изменений

8.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым Положением.
8.2. Настоящее Положение подлежит пересмотру не реже одного раза в три года.

Приложение 1
к Положению о порядке реагирования
на инциденты информационной безопасности

ФОРМА АКТА ОБ ИНЦИДЕНТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АКТ № _____
об инциденте информационной безопасности

г. Москва «» _____ **20** г.

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

В инциденте задействованы следующие работники: _____
(фамилии и инициалы)

Описание инцидента: _____

Причины инцидента: _____

Меры, принятые для устранения причин, последствий инцидента: _____

Администратор информационной безопасности: _____ /_____/
(подпись) (ФИО)

Приложение 2
к Положению о порядке реагирования
на инциденты информационной безопасности

ФОРМА ЖУРНАЛА УЧЁТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Журнал начат: «**»** _____ ***20** г.*
Журнал окончен: «» _____ **20** г.
Ответственный за ведение журнала: _____ /_____/
(ФИО, подпись)

№ п/п	**Краткое описание инцидента**	**ФИО, должность сотрудника, обнаружившего инцидент, дата и время обнаружения**	**Дата и время пресечения несанкционированного воздействия**	**Дата, время доведения информации об инциденте; ФИО, должность сотрудника, принявшего информацию**	**Подпись администратора безопасности**
1					
2					
...					

Приложение 3
к Положению о порядке реагирования
на инциденты информационной безопасности

АКТ
об уничтожении персональных данных, обрабатываемых без средств автоматизации
г. Москва «» _____ 20 г. № _____

Комиссия по уничтожению персональных данных, созданная на основании приказа ректора АНО ДПО «Научный институт профессиональных компетенций» от ___ _____ 20__ г. № __, составила акт о том, что __ ___ 20 г. уничтожила нижеперечисленные носители, содержащие персональные данные, а именно:

№ п/п	Наименование материального носителя, количество листов	Категории уничтоженных персональных данных	Информация о лицах, чьи данные уничтожены	Способ уничтожения	Причина уничтожения
1					
2					
3					

Всего _____
(цифрами и прописью)
Настоящий акт составили:
Председатель комиссии: _____ ///
(ФИО) (подпись) (дата)
Члены комиссии: _____ ///
(ФИО) (подпись) (дата)
_____ ///
(ФИО) (подпись) (дата)
_____ ///
(ФИО) (подпись) (дата)
_____ ///
(ФИО) (подпись) (дата)

Приложение 4
к Положению о порядке реагирования
на инциденты информационной безопасности

АКТ
об уничтожении персональных данных, обрабатываемых с использованием средств автоматизации

г. Москва «» _____ 20 г. № _____

Комиссия по уничтожению персональных данных, созданная на основании приказа ректора АНО ДПО «Научный институт профессиональных компетенций» от ___ _____ 20__ г. № __, составила акт о том, что __ ___ 20 г. уничтожила персональные данные, а именно:

№ п/п	Наименование ИСПДн	Наименование документа	Категория уничтоженных персональных данных	Информация о лицах, чьи данные уничтожены	Способ уничтожения	Причина уничтожения
1						
2						
3						

Всего электронных носителей _____
(цифрами и прописью)
Настоящий акт составили:
Председатель комиссии: _____ ///
(ФИО) (подпись) (дата)
Члены комиссии: _____ ///
(ФИО) (подпись) (дата)
_____ ///
(ФИО) (подпись) (дата)
_____ ///
(ФИО) (подпись) (дата)
_____ ///
(ФИО) (подпись) (дата)

Приложение 5
к Положению о порядке реагирования
на инциденты информационной безопасности

ФОРМА ВЫГРУЗКИ ИЗ ЖУРНАЛА РЕГИСТРАЦИИ СОБЫТИЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наименование ИСПДн	Дата	Событие (уничтожение ПДн)	Категории уничтоженных ПДн	Информация о лицах, чьи данные уничтожены	Причина уничтожения*

* Если ИСПДн не позволяет автоматически отобразить причину уничтожения, ответственный за уничтожение указывает её вручную.