МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный экономический университет»
(УрГЭУ)

П Р И К А З

02.04.2019 № 2/0204-01

г. Екатеринбург

Об утверждении положения о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных

Во исполнение Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных",

П Р И К А З Ы В А Ю:

1. Утвердить и ввести в действие «Положение о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных» (далее - Положение) (Приложение 1).
2. Руководителям структурных подразделений руководствоваться требованиями настоящего положения.
3. Контроль за исполнением настоящего приказа возложить на проректора по управлению имущественным комплексом Кулигина В.А.

И.о. ректора Е.Б. Дворядкина

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный экономический университет»
(УрГЭУ)

УТВЕРЖДЕНО
приказом ректора УрГЭУ
от «02» апреля 2019 г. № 2/0204-01

ПОЛОЖЕНИЕ
О порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных

Екатеринбург
2019

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 работниками УрГЭУ, участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4 В УрГЭУ 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 работников УрГЭУ 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 работников УрГЭУ и (или) иных лиц, нештатного функционирования информационных систем и иных объектов среды информационных активов УрГЭУ, 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.

4. ЦЕЛИ И ЗАДАЧИ ОБРАБОТКИ ИНЦИДЕНТОВ ИБ

Основными целями обработки Инцидентов ИБ являются:

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

3.2. Основными задачами обработки Инцидентов ИБ являются:

- своевременное обнаружение инцидентов ИБ;
- оперативное реагирование на инциденты ИБ;
- координация деятельности работников структурных подразделений УрГЭУ 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 ИБ 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.

5. ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ ИБ

5.1.Обнаружение инцидентов ИБ выполняется работниками УрГЭУ, в том числе с использованием соответствующих технических средств.

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

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

- сообщения работников УрГЭУ;

- сведения, отражённые в журналах регистрации событий информационных систем;
- результаты работы средств защиты информации;
- результаты внутренних проверок;
- другие источники информации об Инцидентах ИБ.

6. ПОРЯДОК АНАЛИЗА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

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

6.2.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.

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

6.4.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.

6.5.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.

6.6.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.

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

7. ОТВЕТСТВЕННОСТЬ

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

7.2. Работники 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
в информационных системах персональных данных

АКТ № ____ (номер вносится в журнал)
об инциденте информационной безопасности

Инцидент зафиксирован

_____
(дата, фамилия и инициалы работника (-ов))

В инциденте задействованы следующие работники

_____
(фамилия и инициалы работника (-ов))
_____

Описание инцидента

_____
_____
_____
_____

Причины инцидента

_____
_____
_____

Меры, принятые для устранения причин, последствий инцидента

_____
_____
_____
_____

Фамилия И.О. «___» _____ 201__ г.

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

_____
(Ф.И.О., подпись)

№ п/п	№ акта	Дата совершения инцидента	Краткое описание инцидента	Сроки устранения инцидента	Ф.И.О. подпись