МОСКОВСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ

MOSCOW INSTITUTE OF TECHNOLOGY AND MANAGEMENT

УТВЕРЖДАЮ:

Ректор ОАНО ВО «МИТУ»

_____М.И. Бородина

«28» октября 2022 г.

ПОЛОЖЕНИЕ О ПОРЯДКЕ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ИНСТИТУТ ТЕХНОЛОГИИ И УПРАВЛЕНИЯ»

(Далее- ОАНО ВО «МИТУ»)

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 ОАНО ВО «МИТУ», участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4 В ОАНО ВО «МИТУ» 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 ОАНО ВО «МИТУ» 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 ОАНО ВО «МИТУ» и (или) иных лиц, нештатного функционирования информационных систем и иных объектов среды информационных активов ОАНО ВО «МИТУ», 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 ИБ, в том числе их закрытия;
- предотвращение и (или) снижение негативного влияния Инцидентов ИБ на осуществление технологических процессов ОАНО ВО «МИТУ»; оперативное совершенствование системы обеспечения информационной безопасности ОАНО ВО «МИТУ».

3.2. Основными задачами обработки Инцидентов ИБ являются:

- своевременное обнаружение инцидентов 1ГБ;
- оперативное реагирование на инциденты ИБ;
- координация деятельности работников структурных подразделений ОАНО ВО «МИТУ» 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 ОАНО ВО «МИТУ», 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 ОАНО ВО «МИТУ»;
- 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