федеральное государственное бюджетное образовательное учреждение высшего образования
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Ректор ФГБОУ ВО ОмГМУ
Минздрава России
_____ М.А. Ливзан
«10» 09 2024 г.

ПОЛОЖЕНИЕ

О РЕГЛАМЕНТЕ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЮ НА НИХ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНО заведующим сектора информационной безопасности Ключенко А.А.

2. ПРИНЯТО ученым советом 19.09.2024 г., протокол № 10.

3. ВВЕДЕНО в действие с 23.09.2024 г. распоряжением от 20.09.2024 г. впервые.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение рассматривает вопросы обнаружения и реагирования на инциденты информационной безопасности (далее – ИБ) в ФГБОУ ВО ОмГМУ Минздрава России (далее – Организации).

1.2 Требования настоящего Положения обязательны для пользователей (далее – Пользователи) и администраторов (далее – Администраторы) информационных систем персональных данных ФГБОУ ВО ОмГМУ Минздрава России.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем Положении использованы ссылки на следующие документы:

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закона от 27 июля 2006 № 152-ФЗ «О персональных данных».

3 ОБЩИЕ ПОЛОЖЕНИЯ

Под инцидентом информационной безопасности понимается любое неблагоприятное событие, в результате которого один из аспектов безопасности может подвергнуться угрозе, слабое место или неисправность системы безопасности.

Реагирование на инциденты безопасности осуществляется в целях:

1) гарантирования целостности информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – Информация).

2) сохранения и восстановления Информации.

3) выяснения причин того, почему инцидент стал возможен.

4) предотвращения развития вторжения и будущих инцидентов.

5) нахождения и наказания нарушителей.

4 ЭТАПЫ РЕАГИРОВАНИЯ НА ИНЦИНДЕНТЫ БЕЗОПАСНОСТИ

Жизненный цикл реагирования на инциденты ИБ состоит из четырех стадий, которые следуют одна за другой и все вместе образуют непрерывный цикл:

1) обнаружение и регистрация инцидента.
2) устранение причин и последствий инцидента.
3) расследование инцидента.
4) реализация корректирующих мероприятий.

Настоящий Регламент должен пересматриваться после каждого инцидента ИБ и по необходимости.

5 ОБНАРУЖЕНИЕ ИНЦИНДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация об инцидентах ИБ может поступать по следующим каналам:

1) журналы регистрации событий операционной системы или средств защиты информации;

2) оповещения подсистемы антивирусной защиты или подсистемы обнаружения (предотвращения) вторжений;

3) информация, получаемая от работников Организации по любым каналам связи (телефон, электронная почта, речевой канал и т.д.).

Все процессы обнаружения инцидентов ИБ подлежат обязательному документированию.

6 ИНФОРМАРИРОВАНИЕ ОБ ИНЦИНДЕНТАХ

Администратор ИБ и совместно с администратором ИС (далее – группа реагирования) отвечают за все процессы по обнаружению и реагированию на

инциденты ИБ. Группа реагирования получает информацию о случившихся инцидентах и принимает меры по их устранению.

Работники, имеющие доступ к системе, в том числе те, кто осуществляет техническое сопровождение данной системы, обязаны при получении информации обо всех нетипичных событиях ИБ, незамедлительно сообщить группе реагирования.

Для оперативного получения информации об инцидентах ИБ группа реагирования имеет следующие каналы связи:

Телефон для обращения в рабочие часы с 8.00 до 16.45 в будние дни:	+7(3812) 20-44-26
Адрес электронной почты:	is@omgmu.ru

К нетипичным событиям ИБ, о которых следует сообщать группе реагирования, относятся:

1. Крахи системы, перезагрузки системы.
2. Появление новых учетных записей.
3. Появление новых файлов.
4. Изменения в размерах и датах файлов.
5. Попытки записи в системные файлы.
6. Модификация или удаление данных (например, начали исчезать файлы).
7. Отказ в обслуживании.
8. Необъяснимо низкая производительность системы (например, необычно плохое время отклика системы).
9. Аномалии (например, появление сообщений на экране, частые и необъяснимые звуковые сигналы).
10. Подозрительные пробы (например, многочисленные неудачные попытки входа с другого узла сети).
11. Ошибки оператора.
12. Несоблюдение политик и руководств по ИБ другими работниками.

13. Нарушение физических мер обеспечения безопасности.

14. Неконтролируемое внесение изменений в систему.

15. Неправильное срабатывание программного или аппаратного обеспечения.

16. Нарушения доступа.

Неправильное срабатывание или другое аномальное поведение системы может стать индикатором атаки на безопасность или нарушения безопасности, и о них надо всегда докладывать, как о случае нарушения информационной безопасности.

Все работники, подрядчики и пользователи третьей стороны должны быть ознакомлены с процедурой информирования об инцидентах нарушения ИБ, а также проинформированы о необходимости незамедлительного сообщения об инцидентах и событиях ИБ.

Группа реагирования проводит сбор информации, связанной с событием, о котором поступило сообщение для того, чтобы убедиться, что инцидент ИБ действительно имеет место быть и локализовать область, задействованную в инциденте.

7 РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ

Для реагирования на инциденты ИБ группа реагирования может привлекать по необходимости работников Организации и внешних экспертов. Необходимость привлечения тех или иных специалистов определяется в зависимости от вида инцидента.

Работники Организации могут привлекаться к реагированию на инциденты ИБ по согласованию с Ректором. Внешние эксперты привлекаются по согласованию с Ректором, при этом в обязательном порядке должно быть заключено письменное соглашение о конфиденциальности между Организацией и внешней стороной.

Все процессы реагирования на инциденты должны обязательно документироваться.

Первостепенной задачей группы реагирования является сдерживание инцидента ИБ, то есть принятие всех необходимых мер для локализации инцидента ИБ, препятствующих его распространению (при этом необходимо ограничить доступ к объектам, задействованным в инциденте ИБ). После сдерживания инцидента группа реагирования должна приступить к ликвидации последствий и восстановлению системы, то есть к приведению системы в нормальное состояние (при этом необходимо протоколировать все действия, которые осуществляются в ходе реагирования на инцидент). Далее группа реагирования проводит расследование инцидента и анализ случившегося.

Целью расследования инцидента ИБ является раскрытие всех причинно-следственных связей и получение следующей информации:

- источники инцидента ИБ (нарушители);
- цели инцидента ИБ;
- способы осуществления инцидента ИБ.

8 АНАЛИЗ ПРИЧИН И ОЦЕНКА РЕЗУЛЬТАТА

После проведения расследования инцидента ИБ группа реагирования проводит:

переоценку рисков, повлекших возникновение инцидента ИБ;

анализ перечня защитных мер для минимизации выявленных рисков в случае повторения инцидента ИБ;

анализ инструкций и правил ИБ, включая настоящий документ;

по необходимости обучение (информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты

информации) персонала Организации для повышения их осведомленности в части ИБ.

Раз в три месяца, а также по необходимости, группа реагирования готовит и предоставляет Ректору отчеты по проведенной работе по расследованию инцидента ИБ с указанием предлагаемых мероприятий, направленных на снижение ущерба от подобных инцидентов ИБ.

ПРИЛОЖЕНИЕ А

Лист ознакомления

с Регламентом выявления инцидентов безопасности и реагированию на них

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Проректор по последипломному образованию
_____ А.С. Колчин
«12» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«11» 09 2024 г.

СОГЛАСОВАНО
Начальник ОА и ИТ
_____ Р.А. Ахмеров
«09» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования
_____ С.В. Плоткина
«12» 09 2024 г.