Утверждаю
Ректор
_____ Л.Н.Горбатова
«26» 05 2021 г.

ПОЛОЖЕНИЕ
о реагировании на инциденты
федерального государственного
бюджетного образовательного
учреждения высшего образования
«Северный государственный медицинский университет»
Министерства здравоохранения Российской Федерации

Версия 2.0

Дата введения: 26.05.2021г.

Архангельск
2021

	Должность	Фамилия/подпись	Дата
Разработал	Директор информационно-интеллектуального центра	Трифонов И.А.	02.04.2021.
Проверил	Начальник управления правового и кадрового обеспечения	Котлов И.А.	02.04.2021.
Согласовал	Первый проректор, проректор по учебно-воспитательной работе	Оправин А.С.	02.04.2021.
	Проректор по цифровой трансформации и инфраструктурному развитию	Халезин А.С.	02.04.2021.

1. Рассмотрено на заседании Ученого совета, протокол № 12 от «14» 04 2021 г.
2. Утверждено и введено в действие приказом Ректора, № 146 от «26» 05 2021 г.
3. Соответствует требованиям СГМУ.
4. Введено в действие взамен Положения о реагировании на инциденты – версия 1.0.

СОДЕРЖАНИЕ

1.ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Целью настоящего Положения является повышение уровня защищенности информационных ресурсов Университета, за счет эффективного управления и определение порядка расследования инцидентов информационной безопасности, своевременное оповещение пользователей вычислительной сети Университета о возникающих угрозах компьютерной безопасности, распространение информации по их предупреждению.

1.2. Процесс расследования и реагирования на инцидент проявляет конкретные уязвимости информационной системы, обнаруживает следы атак и вторжений, а так же проверяется

работа защитных механизмов, качество архитектуры системы обеспечения информационной безопасности и ее управления.

1.3. Процесс управления инцидентами информационной безопасности Университета в виде структурной схемы представлен в Приложении 1.

2.ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

1.1. **Инцидент информационной безопасности** - событие, в результате наступления которого нанесен ущерб ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России (далее - Университет) в виде финансовых потерь, производственных и репутационных рисков (хищение денежных средств со счета, атака на информационные ресурсы Университета, разглашение конфиденциальной информации, нарушение работоспособности автоматизированных систем, внесение несанкционированных изменений, утечка или разглашение персональных данных потребителей и т.д.).

Информационная безопасность - все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности,

доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств её обработки.

Конфиденциальность - свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.

Целостность - неизменность информации в процессе ее передачи или хранения.

Доступность - свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы.

Ущерб - убытки, непредвиденные расходы, утрата имущества и денег, недополученная выгода.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность,

3. ПОРЯДОК РЕГИСТРАЦИИ

3.1. Источником информации об инциденте информационной безопасности может служить следующее:

- сообщения работников, обучающихся, контрагентов Университета направленные в Университет в виде сообщений по электронной почте, служебных записок, заявлений и т.д.
- уведомления/сообщения органов осуществляющих контроль или надзор за деятельностью Университета.

- данные, полученные на основании анализа журналов регистрации информационных систем, систем защиты.

Работники всех структурных подразделений Университета, отвечающие за соответствующие технологические процессы, обязаны при получении информации обо всех нетипичных событиях сообщать в отдел информатизации или ответственному за обеспечение безопасности.

3.2. При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения "обратного" звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).

3.3. Работник, получивший информацию об инциденте, должен сообщить об этом Администратору информационной безопасности и в отдел информатизации. Администратор информационной безопасности сообщает руководителю Университета и руководителю структурного подразделения, в котором случился инцидент.

3.4. Сотрудники отдела информатизации регистрируют полученную информацию в электронном журнале учета инцидентов.

После получения информации работники должны классифицировать инцидент по категории критичности, используя 4 разновидности категорий критичности инцидентов:

1 категория - инцидент может принести к значительным негативным последствиям (ущербу) для информационных активов или репутации Университета.

2 категория - инцидент может принести к негативным последствиям (ущербу) для информационных активов или репутации Университета.

3 категория - инцидент может принести к незначительным негативным последствиям (ущербу) для информационных активов или репутации Университета.

4 категория - инцидент не может принести к негативным последствиям (ущербу) для информационных активов или репутации Университета.

3.5. Все инциденты информационной безопасности должны регистрироваться в электронной системе управления инцидентами. База инцидентов информационной безопасности должна постоянно актуализироваться.

В зависимости от присвоенной категории критичности инцидента происходит определение приоритета и времени реагирования по каждому типу инцидента информационной безопасности. Сопоставление приоритетов и категорий инцидентов информационной безопасности определяется следующим образом:

Очень высокий - соответствует 1 категории. Время реагирования не более 1 часа.

Высокий - соответствует 2 категории. Время реагирования не более 4 часов.

Средний - соответствует 3 категории. Время реагирования не более 8 часов.

Низкий - соответствует 4 категории. Время реагирования не определено.

3.6. В случае регистрации инцидента, в течение рабочего дня работниками отдела информатизации оформляется информационное сообщение (Приложение 2).

4.ПОРЯДОК РАЗБОРА

4.1. Для разбора инцидентов информационной безопасности создается комиссия. В зависимости от приоритета инцидента информационной безопасности, происходит выделение необходимых ресурсов для расследования.

4.2. В состав комиссии могут входить следующие работники Университета:

- ответственные за обеспечение безопасности,
- от отдела информатизации,
- руководитель структурного подразделения, в котором произошел инцидент,
- ответственный за информационную безопасность.

4.3. Комиссия собирает и анализирует все данные об обстоятельствах инцидента (электронные письма, записи информационных систем, показания сотрудников и др.). Проверяются все собранные данные о том, что произошло, когда произошло, кто совершил неприемлемые действия, и как все это может быть предупреждено в будущем.

4.4. Комиссия обязана установить имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

4.5. По окончании разбора инцидента информационной безопасности комиссией оформляется отчет, в котором указываются основные обстоятельства и причины инцидента. Представляется в форме, удобной для принятия решения.

4.6. Отчет предоставляется руководителю Университета, начальнику отдела информатизации, службе безопасности. В конце отчета указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.

4.7. После окончания расследования комиссия принимает решение о наказании виновных лиц, применение защитных механизмов и проведение изменений в процедурах информационной безопасности.

5. АНАЛИЗ ПРИЧИН И ОЦЕНКА РЕЗУЛЬТАТА

После проведения расследования комиссия проводит:

- переоценку рисков, повлекших возникновение инцидента;
- готовит перечень защитных мер для минимизации выявленных рисков, в случае повторения инцидента информационной безопасности;
- актуализирует необходимые политики, регламенты, инструкции по информационной безопасности, включая настоящий документ;
- при необходимости, организует обучение работников Университета для повышения осведомленности в области защиты информации.

Раз в три месяца, начальник отдела информатизации готовит и представляет руководителю Университета отчеты о проведенной работе по расследованию инцидентов информационной безопасности с указанием своей экспертной оценки и проводимыми корректирующими и компенсирующими мероприятиями, направленными на снижение ущерба от подобных инцидентов информационной безопасности.

6. КОНТРОЛЬ ИСПОЛНЕНИЯ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

6.1. Контроль надлежащего исполнения требований настоящего Положения осуществляется начальником отдела информатизации.

7. УТВЕРЖДЕНИЕ И ИЗМЕНЕНИЕ ПОЛОЖЕНИЯ

7.1. Настоящее Положение вводится в действие с момента подписания приказа Ректором.

7.2. Ответственность за соблюдение требований, изложенных в данном Положении, несет Директор ИИЦ.

7.3 Изменения и дополнения в Положение вносятся по инициативе:

- ректора СГМУ;
- первого проректора, проректора по учебно-воспитательной работе;
- проректор по инфраструктурному развитию
- директор ИИЦ;
- начальника управления правового и кадрового обеспечения;

Приложение 2 к Положению(рекомендуемое)

Информационное сообщение

"_____"____20____года Руководителю подразделения

1.Наименование подразделения, ФИО сотрудника, занимаемая должность:
_____
_____
(допустившего отклонения, собирающегося совершить или совершившего операции, попадающие по признакам к сделкам)

2.Реквизиты потребителя или клиента, который является участником операций, выполняемых не в стандартной форме с отклонением от общих норм и правил:
_____
_____
(наименование организации, юридический адрес, тел., ФИО физического лица, паспортные данные, адрес)

3. Факты установленных нарушений или возникших подозрений по поводу возможных отклонений в выполнении операций от установленных стандартов, норм, и правил с указанием предмета сделок, их объемов, даты совершения операций:
_____
_____
_____
_____
_____
Дата составления сообщения: _____
Подпись и ФИО составителя: _____
Дата регистрации поступившего сообщения:_____

Информация о принятых мерах:

_____
_____
_____
_____
_____

"____"_____20_____г.

_____ _____
(подпись) (фамилия и инициалы)

Согласовано: