Приложение 9

УТВЕРЖДЕНО
приказом ГБУЗ "Стоматологическая поликлиника города - курорта Геленджик" МЗ КК
от _____ № _____

ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности в Государственном бюджетном учреждении здравоохранения "Стоматологическая поликлиника города - курорта Геленджик" министерства здравоохранения Краснодарского края

1. Общие положения

Настоящее положение разработано в целях организации работы с инцидентами информационной безопасности в Государственном бюджетном учреждении здравоохранения "Стоматологическая поликлиника города - курорта Геленджик" министерства здравоохранения Краснодарского края (далее – Учреждение).

Инцидент – одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее – ИС) и (или) к возникновению угроз безопасности информации, в том числе персональных данных.

Положение по работе с инцидентами информационной безопасности (далее – Положение) разработано в соответствии с:

1) Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

2) Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;

4) требованиями по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными приказом ФСТЭК России от 18 февраля 2013 г. № 21;

5) требованиями по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждёнными приказом ФСТЭК России от 11 февраля 2013 г. № 17;

6) политикой обработки персональных данных субъектов Учреждения.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

Работа с инцидентами включает в себя следующие направления:

1) определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов;

3) своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

4) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

6) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий; планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в соответствии с приказом и.о. главного врача.

2. Ответственные за выявление инцидентов и реагирование на них

2.1. В информационных системах.

Ответственными за выявление инцидентов в ИС являются:

1) лица, имеющие право доступа к ИС;

2) ответственный за техническое обслуживание ИС (администратор ИС);

3) ответственный за обеспечение безопасности в ИС (администратор ИБ).

Ответственными за реагирование на инциденты в ИС являются:

1) лица, имеющих право доступа к ИС;

2) руководитель подразделения (отдела) Учреждения, в котором выявлен инцидент;

3) ответственный за техническое обслуживание ИС (администратор ИС);

4) ответственный за обеспечение безопасности в ИС (администратор ИБ);

5) ответственный за организацию обработки персональных данных Учреждения, в случае, если ИС является информационной системой персональных данных и (или) государственной (муниципальной) информационной системой, обрабатывающей персональные данные;

6) председатель комиссии по работе с инцидентами.

2.2. Вне информационных систем.

Ответственными за выявление инцидентов вне ИС являются все работники Учреждения.

Ответственными за реагирование на инциденты вне ИС являются:

1) работники Учреждения, обнаружившие инцидент;

2) руководитель структурного подразделения (отдела) Учреждения, в котором выявлен инцидент;

3) ответственный за организацию обработки персональных данных Учреждения, в случае, если существует угроза безопасности персональных данных;

4) председатель комиссии по работе с инцидентами.

3. Обнаружение, идентификация и регистрация инцидентов

3.1. Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

1) выявление инцидентов в области информационной безопасности с помощью технических средств;

2) выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

3) выявление инцидентов с помощью работников Учреждения.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до работников Учреждения информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет председатель комиссии по работе с инцидентами в журнале регистрации инцидентов информационной безопасности. Рекомендуемая типовая форма журнала приведена в приложении к данному документу.

Хранение журнала должна осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение журнала – председатель комиссии по работе с инцидентами.

4. Информирование о возникновении инцидентов

Работник Учреждения (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом сообщить об инциденте непосредственному своему руководителю структурного подразделения (отдела), администратору ИС, администратору ИБ, ответственному за организацию обработки персональных данных в Учреждении, председателю комиссии по работе с инцидентами.

Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и даёт указания по дальнейшим действиям.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее – ПДн), повлекшей нарушение прав субъекта(-ов) ПДн, председатель комиссии по работе с инцидентами уведомляет уполномоченный орган по защите прав субъектов ПДн:

1) в течение 24-х часов – о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет контактные сведения для взаимодействия с комиссией по инцидентам;

2) в течение 72-х часов – о результатах внутреннего расследования выявленного инцидента, а также сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

5.1. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

1) действия организаций и отдельных лиц враждебные интересам Учреждения;

2) отсутствие персональной ответственности работников Учреждения и их непосредственных руководителей за обеспечение информационной безопасности, в том числе персональных данных;

3) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;

4) отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;

5) недостаточная техническая оснащённость структурного подразделения (отдела) или лица, ответственного за обеспечение информационной безопасности;

6) совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;

7) наличие привилегированных бесконтрольных пользователей в информационной системе;

8) пренебрежение правилами и требованиями информационной безопасности работниками Учреждения;

9) и другие причины.

5.2. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

1) определение границ инцидента и ущерба от реализации угроз информационной безопасности;

2) ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

7.1. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

1) планомерной деятельности по повышению уровня осознания информационной безопасности руководством и работниками Учреждения;

2) проведении мероприятий по обучению работников Учреждения правилам и способам работы со средствами защиты информационных систем;

3) доведении до работников норм законодательства, внутренних документов Учреждения, устанавливающих ответственность за нарушение требований информационной безопасности;

4) разъяснительной работе с увольняющимися и принимаемыми на работу работниками Учреждения;

5) своевременной модернизации системы обеспечения информационной безопасности с учётом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности;

6) своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание работников за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал Учреждения является важным источником сведений об инцидентах информационной безопасности, поэтому необходимо донести до работников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности могут являться основанием для смягчения либо отмены наказания за нарушение требований информационной безопасности.

И.о. главного врача Ю.Н. Парасиди