УТВЕРЖДАЮ
Директор
ГКУ РО «УМФЦ»

_____А.В. Алехин

«20» мая 2018 г.

ПОЛИТИКА

по работе с инцидентами информационной безопасности

АННОТАЦИЯ

Настоящая политика разработана в целях выявления, предотвращения и устранения последствий нарушений законодательства Российской Федерации в области обработки персональных данных в соответствии со ст. 18.1 Федерального Закона № 152-ФЗ «О персональных данных».

1. Общие положения

Политика по работе с инцидентами информационной безопасности (далее – Политика) разработана в соответствии с Федеральным Законом № 152-ФЗ «О персональных данных», Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Инциденты в области информационной безопасности возникают при нарушении правил и требований информационной безопасности.

В ходе инцидента реализуются (или создается возможность для реализации) угрозы информационной безопасности, что, как правило, приводит к нанесению вреда активам ГКУ РО «УМФЦ» (далее – Учреждение) и (или) субъекту персональных данных.

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 информационных систем персональных данных.

Работа с инцидентами включает в себя 3 направления:

– выявление инцидентов в области информационной безопасности;

– реакция на инциденты в области информационной безопасности;

– предупреждение инцидентов в области информационной безопасности.

2. Выявление инцидентов в области информационной безопасности

Работа по выявлению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

– выявление инцидентов в области информационной безопасности с помощью технических средств;

– выявление инцидентов в области информационной безопасности в ходе мероприятий по контролю за обработкой персональных данных;

– выявление инцидентов с помощью персонала Учреждения.

3. Реакция на инциденты в области информационной безопасности

Реакция на инциденты в области информационной безопасности включает в себя:

– фиксацию инцидента в области информационной безопасности;

– определение границ инцидента и ущерба (в том числе потенциального) от реализации угроз информационной безопасности в ходе инцидента;

– ликвидация последствий инцидента и полное либо частичное возмещение ущерба;

– наказание виновных в инциденте информационной безопасности.

4. Предупреждение инцидентов в области информационной безопасности

Предупреждение инцидентов строится на:

– планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками Учреждения;

– проведения мероприятий по обучению сотрудников Учреждения правилам и способам работы со средствами защиты информационных систем персональных данных;

– доведении до сотрудников норм законодательства в области защиты персональных данных и внутренних документов Учреждения, устанавливающих ответственность за нарушение требований информационной безопасности;

– разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимающимися на работу;

– своевременной модернизации системы обеспечения информационной безопасности информационных систем персональных данных с учетом возникновения новых угроз информационной безопасности;

– своевременном обновлении программного обеспечения, в т.ч. баз сигнатур антивирусных средств.

4.1. Причины инцидентов в области информационной безопасности

Причинами инцидентов в области информационной безопасности являются:

– действие враждебных интересам Учреждения организаций и отдельных лиц;

– отсутствие персональной ответственности за обеспечение информационной безопасности персональных данных сотрудников Учреждения и их руководителей;

– недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности персональных данных;

– отсутствие моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;

– недостаточная техническая оснащенность подразделений, ответственных за обеспечение информационной безопасности;

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

– наличие привилегированных бесконтрольных пользователей в информационной системе;

– пренебрежение правилами и требованиями информационной безопасности сотрудниками Учреждения;

– и другие причины.

4.2. Расследование инцидентов в области информационной безопасности

Расследование инцидентов в области информационной безопасности должно включать в себя:

– формирование комиссии по расследованию инцидента в области информационной безопасности;

– определение границ инцидента – информационных ресурсов, технических средств и персонала, затронутых инцидентом;

– определение причин инцидента, факторов, влияющих на возникновение инцидента;

– определение участников инцидента;

– определение последствий инцидента;

– составление заключения по результатам расследования;

– выработка рекомендаций по предотвращению возникновения подобных инцидентов в будущем.

4.3. Работа с персоналом по предупреждению инцидентов

Как правило, самым слабым звеном в любой системе безопасности является человек. Наличие современных доступных способов воздействия на персонал

Учреждения, таких как социальная инженерия, фишинг, подмена электронных идентификаторов, номеров телефонов и т.д., делает пользователя информационной системы персональных данных частым объектом внимания злоумышленника. Поэтому направление работы с персоналом является основным направлением работы подразделений информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника 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 так же важным источником сведений об инцидентах информационной безопасности. Поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются поводом для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Частой причиной инцидентов информационной безопасности является личная обида подчиненных на своих руководителей, либо коллег. Поэтому благоприятный микроклимат в коллективе является необходимым фактором обеспечения информационной безопасности в организации.