|  |  |
| --- | --- |
|  | Приложение 19к приказу комитетапо культуре города Барнаулаот 29 июля 2021г. №64 |

РЕГЛАМЕНТ

ответственного за обеспечение безопасности информации в информационных системах

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

КИ – конфиденциальная информация.

ИС – информационная система.

ГИС – государственная информационная система.

ИСПДн – информационная система персональных данных.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС, в том числе ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения

1.1. Регламент ответственного за обеспечение безопасности информации в информационных системах (далее - Регламент) в ИС общего пользования, ГИС, ИСПДн, ИС, содержащих другие виды КИ, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к ключевым системах информационной инфраструктуры (далее – Инструкция) определяет основные права и обязанности ответственного за обеспечение безопасности информации в комитете по культуре города Барнаула (далее –комитет).

1.2. Ответственное лицо за обеспечение безопасности информации назначается приказом Председателя комитета по культуре города Барнаула на основании Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» может быть назначено несколько ответственных в зависимости от защищаемой информации.

1.3. Ответственное лицо за обеспечение безопасности информации (АИБ) – лицо, отвечающее за организацию и состояние процесса обеспечения безопасности обработки информации в ИС, в том числе ИСПДн (далее – ИС).

1.4. АИБ проводит свою работу согласно нормативным методическим документам ФСТЭК России, ФСБ России и иных уполномоченных законодательством органов в области обеспечения безопасности информации.

1.5. АИБ назначается из числа сотрудников комитета по культуре города Барнаула, обладающих определенными знаниями в области защиты информации.

1.6. Работа АИБа проводится в соответствии с планом работ, утвержденным решением председателя комитета.

1.7. В своей работе АИБ руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности информации и нормативными правовыми актами комитета по обеспечению безопасности информации.

2. Обязанности администратора информационной безопасности

2.1. АИБ обязан:

2.1.1. проводить мероприятия по организации обеспечения безопасности информации, включая установление уровней защищенности систем персональных данных, классификацию ГИС, медицинских информационных систем, ИС общего пользования, автоматизированных систем;

2.1.2. проводить мероприятия по техническому обеспечению безопасности информации при ее обработке в ИС, в том числе:

мероприятия по охране, организации доступа в помещения, где ведется обработка;

мероприятия по закрытию технических каналов утечки при их обработке;

мероприятия по защите от несанкционированного доступа;

мероприятия по выбору средств защиты.

2.1.3. Проводить мероприятия, направленные на предотвращение передачи информации лицам, не имеющим права доступа к такой информации.

2.2. Обеспечивать недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено их функционирование.

2.3. Осуществлять постоянный контроль за обеспечением уровня защищенности персональных данных, класса защищенности ГИС, медицинских информационных систем, ИС общего пользования, автоматизированных систем и пр., за соблюдением пользователями режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации.

2.4. Участвовать в подготовке объектов комитета по культуре города Барнаула к оценке эффективности реализованных в рамках системы защиты мер по обеспечению безопасности.

2.5. Разрабатывать организационно-распорядительные документы по обеспечению безопасности информации в комитете.

2.6. Проводить периодический контроль эффективности мер защиты информации в комитете.

2.7. Организовывать в установленном порядке изучение причин и условий появления нарушений в безопасности информации и осуществлять разработку предложений по устранению недостатков и предупреждению подобного рода нарушений.

2.8. Разрабатывать предложения и участие в проводимых работах по совершенствованию системы безопасности информации в комитете.

2.9. Осуществлять ознакомление специалистов с законодательством в сфере обработки и защиты информации, а также с локальными нормативными правовыми актами комитета по данному вопросу.

2.10. Оказывать методическую помощь по вопросам обеспечения безопасности информации сотрудникам комитета.

2.11. Осуществлять подготовку отчетов о состоянии работ по обеспечению безопасности информации в комитете.

2.12. Осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных (выходных) документов, содержащих защищаемую информации.

2.13. Контролировать порядок использования и обеспечения сохранности персональных устройств идентификации пользователей.

3. Права администратор информационной безопасности

3.1. АИБ имеет право:

требовать от всех пользователей ИС выполнения установленной технологии обработки информации, инструкций и других нормативных правовых документов по обеспечению безопасности информации;

запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности информации;

разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности информации;

готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации;

пользоваться необходимой помощью специалистов из числа сотрудников комитета для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности информации;

инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических средств из состава информационных систем;

обращаться к председателю комитета по культуре с предложением о приостановке процесса обработки информации или отстранению от работы пользователя в случаях нарушения установленной технологии обработки информации или нарушения режима конфиденциальности;

подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты информации в комитете.

4. Ответственность администратор информационной безопасности

4.1. АИБ несет персональную ответственность за:

правильность и объективность принимаемых решений;

правильное и своевременное выполнение распоряжений и указаний председателя комитета, ответственного за организацию обработки информации по вопросам, входящим в возложенные на него функции;

правильное и своевременное выполнение организационных и распорядительных документов, принятых комитете по вопросам обработки и защиты информации;

выполнение возложенных на него обязанностей, предусмотренных Регламентом;

качество проводимых работ по обеспечению безопасности информации в соответствии с функциональными обязанностями;

согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы;

соблюдение трудовой дисциплины, охраны труда.