|  |
| --- |
| Приложение  к приказу комитета  от 13.05.2022 №93 |

ПОЛОЖЕНИЕ   
об обеспечении безопасности общедоступной информации   
в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула

1. Общие положения

1. Положение об обеспечении безопасности общедоступной информации в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула (далее - Положение) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой и защитой информации.
2. Настоящее положение устанавливает требования к обеспечению безопасности общедоступной информации в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула (далее - ИС), доступ к которой не ограничен федеральными законами.

Под ИС понимается - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, расположенных в помещениях комитета по финансам, налоговой и кредитной политике города Барнаула (далее – Комитет) по адресу: г. Барнаул, ул. Ленина, 6.

ИС используются для хранения, обработки и передачи информации, в соответствии с функциями, возложенными на Комитет.

ИС включает в себя:

* аппаратно-программный комплекс серверной группы Комитета (далее - Серверная группа);
* рабочие станции, сетевое оборудование, периферийное оборудование (принтеры, сканеры и т.п.) и другое специализированное оборудование Комитета.

1. Безопасность общедоступной информации, при ее обработке в ИС, обеспечивается применением организационных мер и технических средств защиты информации, реализующих требования нормативных правовых актов Российской Федерации.
2. Требования настоящего Положения и других документов, разработанных для их реализации, являются обязательными для исполнения всеми лицами, получившими доступ к общедоступной информации в ИС Комитета, и должны быть доведены до их сведения.
3. Решение о необходимости внесения изменений в Положение принимается на основании:

* изменения нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой и защитой информации;
* результатов анализа инцидентов информационной безопасности в информационных системах;
* изменения технологии обработки информации.

2. Цель защиты информации и основные виды угроз безопасности

1. Основной целью Положения является обеспечение принятия организационных и технических мер, направленных на:

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализацию права на доступ к информации.

1. На основании Положения устанавливаются требования:

* разграничения доступа к общедоступной информации, порядка и условий такого доступа;
* обработки информации;
* передачи информации другим лицам по договору или на ином установленном законом основании;

1. Основными видами угроз безопасности общедоступной информации в ИС являются:

* противоправные и (или) ошибочные действия пользователей информационных систем и третьих лиц;
* отказы, сбои программного обеспечения и технических средств информационных систем, приводящие к модификации, блокированию, уничтожению, а также нарушению правил эксплуатации персональных электронно-вычислительных машин (далее – ПЭВМ);
* стихийные бедствия, техногенные аварии, сбои и отказы технических средств информационных систем.

3. Методы и способы защиты общедоступной информации в ИС

3.1. Для достижения основной цели защиты информации, системы безопасности информации обеспечивают эффективное решение следующих задач:

* предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;
* своевременное обнаружение фактов несанкционированного доступа;
* предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
* недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
* возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
* постоянный контроль за обеспечением защищенности информации.
* нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.
  1. Для выполнения требований настоящего Положения утверждаются:
* порядок организации парольной защиты в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула (приложение 1);
* порядок проведения антивирусного контроля в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула (приложение 2);
* порядок технического обслуживания, ремонта, модернизации технических средств, входящих в состав информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула (приложение 3);
* регламент по работе пользователей в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула (приложение 4);
* регламент резервного копирования информации в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула (приложение 5);
* положение о разрешительной системе допуска к информационным системам персональных данных в комитете по финансам, налоговой и кредитной политике города Барнаула (приложение 6).
  1. Охрана помещений, в которых ведется обработка информации и организация режима безопасности в этих помещениях, обеспечивает сохранность технических средств ИС, носителей информации и средств защиты информации, а также исключение возможности неконтролируемого пребывания посторонних лиц в этих помещениях.

4. Обязанности

1. Отдел внедрения автоматизированных систем финансовых расчетов комитета:

* определяет порядок доступа пользователей к общедоступной информации, расположенной в информационных ресурсах Серверной группы;
* отвечает за разграничение доступа к общедоступной информации, расположенной в информационных ресурсах Серверной группы.
* отвечает за своевременное обнаружение фактов несанкционированного доступа к ИС;
* разрабатывает предложения по дальнейшему совершенствованию системы защиты информации, планируют мероприятия по защите ИС;
* организует проведение мероприятий по защите информации с привлечением комитета информатизации города Барнаула:
* обеспечивает защиту общедоступной информации, расположенной в Серверной группе;
* осуществляет администрирование Серверной группы;
* обеспечивает проведение антивирусного контроля информации, расположенной в Серверной группе;
* осуществляет резервное копирование и восстановление информации расположенной в Серверной группе;
* сопровождает функционирование программного обеспечения рабочих станций ИС;
* организует техническое обслуживание рабочих станций, периферийного и другого специализированного оборудования;
* в случае необходимости удаленно контролирует состояние рабочих станций;
* организует работы по проведению антивирусного контроля рабочих станций.
* отвечает за соблюдение в ИС требований по обеспечению безопасности информации.

1. Пользователь ИС - сотрудник, допущенный к работе в ИС:

* отвечает за соблюдение установленного порядка использования программного обеспечения, а также применение технических и программных средств ИС;
* соблюдает требования нормативных документов по обеспечению безопасности информации, обрабатываемой в ИС;
* соблюдает утвержденную разрешительную систему доступа к техническим средствам ИС и информации, обрабатываемой в ИС;
* не имеет права на изменение компонентов ПЭВМ, отключение или изменение настроек антивирусной защиты.

5. Ответственность

* 1. Ответственность за реализацию и соблюдение требований Положения пользователями ИС, возлагается на начальников отделов и ответственных специалистов Комитета.
  2. Нарушение требований Положения влечет за собой дисциплинарную, административную и иную ответственность в соответствии с действующим законодательством Российской Федерации.