Комитет администрации Ельцовского района по финансам, налоговой и кредитной политике

Приказ

18.09.2017 с. Ельцовка № 08

Об утверждении положения обеспечении безопасности общедоступной информации в информационных системах Комитета администрации Ельцовского района по финансам, налоговой и кредитной политике

В целях реализации положений Конституции Российской Федерации, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» постановляю:

1. Утвердить положение об обеспечении безопасности общедоступной информации в информационных системах Комитета администрации Ельцовского района по финансам, налоговой и кредитной политике.

2. Контроль исполнения настоящего постановления возложить на начальника информационного отдела Жигадло Ю. А.

Председатель комитета Н. В. Старовойтова

УТВЕРЖДЕН
приказом Комитета администрации
Ельцовского района по финансам,
налоговой и кредитной политике
от 18.09.2017 № 08

ПОЛОЖЕНИЕ
об обеспечении безопасности общедоступной информации в информационных системах Комитета администрации Ельцовского района по финансам, налоговой и кредитной политике

1. Общие положения

1.1. Типовое положение об обеспечении безопасности общедоступной информации в информационных системах органов исполнительной власти Алтайского края, органов местного самоуправления Алтайского края и подведомственных им организаций (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.

1.2. Настоящее положение устанавливает требования к обеспечению безопасности общедоступной информации в информационных системах органов исполнительной власти Алтайского края, органов местного самоуправления Алтайского края и подведомственных им организаций (далее – «ИС»), доступ к которой не ограничен федеральными законами.

Под ИС понимается совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий, технических средств органов исполнительной власти Алтайского края, органов местного самоуправления Алтайского края и подведомственных им организаций (далее – «организация»).

ИС используются для хранения, обработки и передачи информации в соответствии с функциями организации.

ИС включают в себя аппаратно-программный комплекс серверной группы, рабочие станции, сетевое оборудование, периферийное оборудование (принтеры, сканеры и т.п.) и другое специализированное оборудование организации.

1.3. Безопасность общедоступной информации при ее обработке в ИС обеспечивается применением организационных мер и технических средств защиты информации, реализующих требования нормативных правовых актов Российской Федерации.

1.4. Требования настоящего положения и других документов, разработанных для их реализации, являются обязательными для исполнения всеми лицами, получившими доступ к общедоступной информации в ИС, и

должны быть доведены до их сведения.

1.5. 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 ИС;

изменения технологии хранения и обработки информации.

1.6. Все изменения положения до их ввода в действие подлежат предварительной оценке на соответствие нормативным правовым актам и нормативным методическим документам Российской Федерации, регулирующим отношения, связанные с обработкой и защитой информации.

2. Цель защиты информации и основные виды угроз безопасности

2.1. 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;

реализацию права на доступ к информации.

2.2. На основании положения устанавливаются требования к:

разграничению доступа к общедоступной информации, порядку и условиям такого доступа;

порядку хранения и обработки информации;

передаче информации другим лицам по договору или на ином установленном законом основании;

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

противоправные и (или) ошибочные действия пользователей ИС и третьих лиц;

отказы, сбои программного обеспечения и технических средств ИС, приводящие к модификации, блокированию, уничтожению, а также нарушению правил эксплуатации ПЭВМ;

стихийные бедствия, техногенные аварии, сбои и отказы технических средств ИС.

3. Методы и способы защиты общедоступной информации в ИС

3.1. Для достижения основной цели защиты информации системы безопасности должны обеспечивать 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;

создание возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением защищенности информации.

3.2. Для выполнения требований настоящего положения утверждаются:

инструкция по проведению антивирусного контроля в ИС;

инструкция по организации парольной защиты в ИС;

инструкция по организации обслуживания и ремонта технических средств ИС;

инструкция по работе пользователей в ИС;

инструкция по организации резервного копирования информации в ИС;

типовая форма журнала учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа.

3.3. Охрана помещений, в которых ведется обработка информации и организация режима безопасности в этих помещениях, должна обеспечивать сохранность технических средств ИС, носителей информации и средств защиты информации, а также исключение возможности неконтролируемого пребывания посторонних лиц в этих помещениях.

4. Обязанности

4.1. Руководитель организации:

организует работу сотрудников организации в ИС;

утверждает расходы на финансовое, материально–техническое и иное обеспечение мероприятий по функционированию ИС.

4.2. Подразделение или лицо, ответственное за защиту информации в организации:

организует защиту общедоступной информации, расположенной в ИС;

определяет порядок доступа к общедоступной информации, расположенной в ИС;

осуществляет методическое руководство и внесение предложений по организации и совершенствованию систем защиты информации;

отвечает за соблюдение в ИС требований по обеспечению безопасности информации;

отвечает за своевременное обнаружение фактов несанкционированного доступа к ИС.

4.3. Подразделение или лицо, ответственное за администрирование ИС в организации:

осуществляет администрирование ИС;

сопровождает функционирование программного обеспечения рабочих станций ИС;

в случае необходимости удаленно контролирует состояние рабочих станций;

организует и обеспечивает работы по проведению антивирусного контроля ПЭВМ.

осуществляет резервное копирование и восстановление информации, расположенной в ИС.

4.4. Подразделение или лицо, ответственное за техническое обслуживание средств вычислительной техники в организации:

организует обслуживание технических средств ИС, периферийного и другого специализированного оборудования;

обеспечивает анализ и устранение неисправностей технических средств и ПО, предпринимает необходимые действия по их предупреждению.

4.5. 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 разрешительную систему доступа к техническим средствам ИС и информации, обрабатываемой в ней;

не имеет права на изменение компонентов ПЭВМ, отключение или изменение настроек антивирусной защиты.

5. Ответственность

5.1. Ответственность за реализацию и соблюдение требований положения пользователями ИС возлагается на начальников структурных подразделений и ответственных лиц организации.

5.2. Нарушение требований положения влечет ответственность в соответствии с действующим законодательством Российской Федерации.