УПРАВЛЕНИЕ
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
АЛТАЙСКОГО КРАЯ

ПРИКАЗ

21 сентября 2017 г. Барнаул № 113

Об утверждении Положения об обеспечении безопасности общедоступной информации в информационных системах управления связи и массовых коммуникаций Алтайского края

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в целях обеспечения безопасности информационных систем управления связи и массовых коммуникаций Алтайского края п р и к а з ы в а ю:

1. Утвердить Положение об обеспечении безопасности общедоступной информации в информационных системах управления связи и массовых коммуникаций Алтайского края.

2. Отделу информационной безопасности (Канаев А.А.) обеспечить ознакомление государственных гражданских служащих и работников управления связи и массовых коммуникаций Алтайского края с утвержденным пунктом 1 настоящего приказа Положением.

3. Признать утратившим силу приказ управления информационных технологий и связи Алтайского края от 18.03.2015 № 16 «Об обеспечении безопасности информационных систем управления информационных технологий и связи Алтайского края».

4. Контроль за исполнением настоящего приказа возложить на заместителя начальника управления, начальника отдела развития информационных систем и ресурсов Переверзева М.В.

Начальник управления М.В. Герасимюк

УТВЕРЖДЕНО

приказом управления связи и массовых коммуникаций Алтайского края
от 21.09.2017 № 113

ПОЛОЖЕНИЕ
об обеспечении безопасности общедоступной информации в информационных системах управления связи и массовых коммуникаций Алтайского края

1. Общие положения

1.1. Положение об обеспечении безопасности общедоступной информации в информационных системах управления связи и массовых коммуникаций Алтайского края (далее – «Положение») разработано в соответствии с 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 управления связи и массовых коммуникаций Алтайского края (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 управления связи и массовых коммуникаций Алтайского края (далее – «Управление»).

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

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

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, регулирующих отношения, связанные с обработкой и защитой информации.

1.4. Требования настоящего Положения и других документов по защите информации, разработанных для его 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.

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;

на реализацию права пользователей ИС на доступ к информации.

2.2. На основании Положения устанавливаются требования:

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

к порядку хранения и обработки информации;

к передаче информации другим лицам по договору или на ином законном 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. В целях защиты информации от неправомерного или случайного доступа, блокирования или изменения система безопасности должна 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. Выполнение требований настоящего Положения предполагает организацию деятельности Управления в соответствии со следующими докумен-

тами:

Инструкция по работе пользователей в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации парольной защиты в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации резервного копирования информации в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по проведению антивирусного контроля в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа;

Инструкция по организации обслуживания и ремонта технических средств в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации доступа в помещения управления связи и массовых коммуникаций Алтайского края, в которых осуществляется обработка защищаемой информации, в том числе персональных данных и иной информации конфиденциального характера;

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. Ответственные лица (структурные подразделения) Управления

4.1. Начальник Управления:

организует работу государственных гражданских служащих и работников Управления в ИС;

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

4.2. Отдел информационной безопасности Управления:

организует защиту общедоступной информации, расположенной в ИС;

определяет порядок доступа к общедоступной информации, расположенной в ИС;

осуществляет периодический контроль за соблюдением порядка доступа к общедоступной информации, расположенной в ИС;

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

обеспечивает соблюдение в ИС требований по обеспечению безопасности

информации;

обеспечивает своевременное обнаружение фактов несанкционированного доступа к ИС.

4.3. Отдел администрирования Управления:

осуществляет администрирование ИС;

сопровождает функционирование программного обеспечения рабочих станций ИС;

организует обслуживание технических средств 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. Отдел правовой и кадровой работы Управления уведомляет отдел администрирования об изменении кадрового состава Управления.

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 средств защиты информации.

5. Заключительные положения

5.1. Нарушение требований Положения влечет ответственность согласно действующему законодательству Российской Федерации.

5.2. Настоящее Положение не заменяет собой действующее законодательство Российской Федерации, регулирующее отношения, связанные с обеспечением безопасности информации.