УПРАВЛЕНИЕ
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
АЛТАЙСКОГО КРАЯ

ПРИКАЗ

21 сентября 2017 № 111

г. Барнаул

Об утверждении Положения об обеспечении безопасности информации конфиденциального характера в управлении 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 приказываю:

1. Утвердить прилагаемое Положение об обеспечении безопасности информации конфиденциального характера в управлении связи и массовых коммуникаций Алтайского края.

2. Отделу информационной безопасности (Канаев А.А.) обеспечить ознакомление сотрудников управления связи и массовых коммуникаций Алтайского края с настоящим приказом.

3. Признать утратившим силу приказ управления информационных технологий и связи Алтайского края от 18.11.2015 № 38 «Об утверждении Положения об обеспечении безопасности информации конфиденциального характера, обрабатываемой в информационных системах 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 № 111

ПОЛОЖЕНИЕ
об обеспечении безопасности информации конфиденциального характера в управлении связи и массовых коммуникаций Алтайского края

1. Общие положения

1.1. Положение об обеспечении безопасности информации конфиденциального характера в управлении 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», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282 (далее – СТР-К), а также на основании других нормативных правовых актов, методических документов Российской Федерации, регулирующих отношения, связанные с обработкой и защитой информации конфиденциального характера.

1.2. Перечень сведений конфиденциального характера утверждается приказом управления связи и массовых коммуникаций Алтайского края (далее – «Управление») с учетом требования законодательства Российской Федерации.

1.3. Настоящее Положение устанавливает требования к обеспечению безопасности информации конфиденциального характера, обрабатываемой в информационных системах и защищаемых помещениях Управления.

Под информационной системой (далее – ИС) понимается совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Под защищаемым помещением (далее – ЗП) понимается помещение, специально предназначенное для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и прочее).

1.4. Безопасность информации конфиденциального характера при ее обработке в ИС и ЗП обеспечивается применением организационных и технических мер.

1.5. Требования настоящего Положения являются обязательными для исполнения всеми сотрудниками Управления, получившими доступ к информации конфиденциального характера, и должны быть доведены до их сведения.

1.6. Решение о необходимости внесения изменений в Положение принимается на основании:

изменения нормативных правовых актов и методических документов,

регулирующих отношения, связанные с обработкой и защитой информации конфиденциального характера;

результатов анализа инцидентов информационной безопасности в Управлении;

изменения технологии хранения и обработки информации конфиденциального характера.

2. Цели и задачи защиты информации

2.1. Основными целями защиты информации являются:

обеспечение защиты информации от несанкционированного доступа, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации;

реализация права на доступ к конфиденциальной информации.

2.2. Цели, указанные в пункте 2.1 Положения, достигаются путем выполнения следующих задач:

определение порядка работы пользователей в ИС Управления;

обеспечение парольной защиты ИС Управления;

обеспечение антивирусной защиты ИС Управления;

организация резервного копирования информации в ИС Управления;

определение порядка обращения с носителями информации, предназначенной для обработки и хранения информации ограниченного доступа;

организация обслуживания и ремонта технических средств в ИС Управления;

организация доступа в помещения Управления, в которых ведется обработка информации конфиденциального характера;

обеспечение безопасности информации конфиденциального характера, обрабатываемой в ЗП.

3. Методы и способы защиты информации конфиденциального характера, обрабатываемой в ИС

3.1. Для обеспечения защиты информации конфиденциального характера применяются методы и способы защиты информации, которые должны обеспечивать эффективное решение следующих задач:

предотвращение несанкционированного доступа к информации конфиденциального характера 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 конфиденциального характера;

недопущение воздействия на технические средства обработки информации конфиденциального характера, в результате которого нарушается их функционирование;

создание возможности восстановления информации конфиденциально-

го характера, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением защищенности информации конфиденциального характера.

3.2. Требования настоящего Положения выполняются в соответствии со следующими документами:

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. Обработка документов с пометкой «Для служебного пользования» допускается только в ИС, аттестованных по требованиям безопасности информации.

4. Методы и способы защиты информации конфиденциального характера, обрабатываемой в ЗП

4.1. В соответствии с установленными требованиями по защите информации в Управлении определяется перечень ЗП и лиц, ответственных за их эксплуатацию, а также составляется технический паспорт на ЗП.

4.2. ЗП размещаются в контролируемой зоне (далее – КЗ) Управления. При этом рекомендуется размещать их с учетом положений СТР-К.

4.3. ЗП оснащаются сертифицированными по требованиям безопасности информации основными и вспомогательными техническими средствами, и системами (далее – ОТСС и ВТСС) или соответствующими средствами защиты. Эксплуатация ОТСС и ВТСС, а также средств защиты должна осуществляться в соответствии с эксплуатационной документацией на них.

4.4. Специальная проверка ЗП и установленного в нем оборудования с целью выявления возможно внедренных в них электронных устройств съема информации (закладных устройств) проводится по решению начальника Управления.

4.5. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, оконечных устройств беспроводной связи, незащищенных переносных диктофонов и других средств аудио- и видеозаписи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также телефонных аппаратов с автоматическим определителем номера, их следует отключать от сети на время проведения обозначенных мероприятий или использовать соответствующие средства защиты.

4.6. Для исключения возможности утечки информации за счет электроакустического преобразования рекомендуется оконечные устройства телефонной связи, имеющие прямой выход в городскую автоматическую телефонную станцию (далее – АТС), оборудовать сертифицированными средствами защиты от утечки за счет электроакустического преобразования.

4.7. Для исключения возможности скрытного подключения к телефонной сети и прослушивания ведущихся в ЗП разговоров не рекомендуется устанавливать в них цифровые телефонные аппараты цифровых АТС, имеющих выход в городскую АТС или к которой подключены абоненты, не являющиеся сотрудниками Управления.

В случае необходимости рекомендуется использовать сертифицированные по требованиям безопасности информации цифровые АТС либо устанавливать в эти ЗП аналоговые аппараты или цифровые телефонные аппараты с вмонтированными в них сертифицированными средствами защиты, либо временно отключать их от телефонной сети.

4.8. Системы пожарной и охранной сигнализации ЗП должны строиться только по проводной схеме связи с пультом.

В качестве оконечных устройств пожарной и охранной сигнализации в ЗП рекомендуется использовать изделия, сертифицированные по требованиям безопасности информации.

4.9. Звукоизоляция ограждающих конструкций ЗП, их систем вентиляции и кондиционирования в местах возможного перехвата информации должна исключать возможность прослушивания ведущихся в нем разговоров за пределами ЗП.

Если предложенными выше методами не удается обеспечить необходимую акустическую защиту, следует применять организационные меры, ограничивая на период проведения конфиденциальных мероприятий доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в ЗП.

4.10. Для снижения вероятности перехвата информации по виброакустическому каналу организационными мерами исключается возможность установки посторонних (внештатных) предметов на внешней стороне ограждающих конструкций ЗП и выходящих из них инженерных коммуникаций

(систем отопления, вентиляции, кондиционирования).

Для снижения уровня виброакустического сигнала расположенные в ЗП элементы инженерно-технических систем отопления, вентиляции оборудуются звукоизолирующими экранами.

4.11. Если при проведении технического контроля обнаружено, что указанные выше меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны или нецелесообразны, то рекомендуется применять метод активного акустического или виброакустического маскирующего зашумления.

Для этой цели должны применяться сертифицированные средства активной защиты.

4.12. При эксплуатации ЗП предусматриваются организационные меры, направленные на исключение несанкционированного доступа в помещение:

двери ЗП в период между мероприятиями, а также в нерабочее время необходимо запирать на ключ;

выдача ключей от ЗП должна производиться лицам, работающим в нем или ответственным за это помещение;

установка и замена оборудования, мебели, ремонт ЗП должны производиться только по согласованию и под контролем подразделения (специалиста) по защите информации.

5. Обязанности сотрудников Управления

5.1. Сотрудники отдела информационной безопасности:

организуют защиту информации конфиденциального характера, обрабатываемой в ИС и ЗП;

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

отвечают за соблюдение требований по обеспечению безопасности информации, обрабатываемой в ИС и ЗП;

отвечают за обнаружение фактов несанкционированного доступа к ИС и в ЗП;

организуют аттестацию по требованиям безопасности информации ИС, предназначенных для обработки документов с пометкой «Для служебного пользования»;

организуют аттестацию ЗП;

осуществляют администрирование ИС, аттестованных по требованиям безопасности информации;

организуют и обеспечивают работы по проведению антивирусного контроля ИС, аттестованных по требованиям безопасности информации;

осуществляют резервное копирование и восстановление информации конфиденциального характера, обрабатываемой в ИС, аттестованных по требованиям безопасности информации.

5.2. Сотрудники отдела администрирования:

сопровождают функционирование программного обеспечения ИС;

проводят обслуживание ИС, периферийного и другого специализированного оборудования.

5.3. Сотрудники отдела правовой и кадровой работы уведомляют сотрудников отдела информационной безопасности об изменении кадрового состава Управления.

5.4. Пользователи ИС:

отвечают за соблюдение установленного порядка использования ИС;

соблюдают требования нормативных документов по обеспечению безопасности информации конфиденциального характера, обрабатываемой в ИС;

соблюдают порядок доступа к ИС и информации конфиденциального характера, обрабатываемой ими;

осуществляют обработку документов с пометкой «Для служебного пользования» в аттестованных по требованиям безопасности информации ИС.

5.5. Сотрудники Управления, работающие в ЗП:

соблюдают требования по обеспечению безопасности информации конфиденциального характера, обрабатываемой в ЗП;

соблюдают порядок доступа в ЗП и к информации конфиденциального характера, обрабатываемой в них.

6. Ответственность

6.1. Ответственность за реализацию и соблюдение требований Положения возлагается на начальников структурных подразделений, пользователей ИС, сотрудников Управления, работающих в ЗП, и ответственных лиц Управления.

6.2. Нарушение требований Положения влечет ответственность в соответствии с действующим законодательством Российской Федерации.

7. Контроль состояния защиты информации конфиденциального характера

7.1. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности информации конфиденциального характера при обработке в ИС и ЗП осуществляется ФСТЭК России, ФСБ России в пределах их полномочий и без права ознакомления с информацией конфиденциального характера, обрабатываемой в ИС и ЗП.

7.2. Повседневный контроль принятия организационных и технических мер, направленных на обеспечение защиты информации конфиденциального характера при обработке в ИС и ЗП, осуществляется сотрудниками отдела информационной безопасности, в помещении режимно-секретного подразделения – главным специалистом сектора спецработы и кадров отдела правовой и кадровой работы.