АДМИНИСТРАЦИЯ АЛТАЙСКОГО КРАЯ

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ АЛТАЙСКОГО КРАЯ

ПРИКАЗ

07 июля 2016 № 55

г. Барнаул

Об утверждении Положения
об удостоверяющем центре
Алтайского края

Во исполнение распоряжения Администрации края от 08.06.2016 № 165-р п р и к а з ы в а ю:

1. Утвердить прилагаемое Положение об удостоверяющем центре Алтайского края.

2. Возложить функции удостоверяющего центра Алтайского края на отдел информационной безопасности управления информационных технологий и связи Алтайского края.

3. Контроль за исполнением настоящего приказа возложить на заместителя начальника управления, начальника отдела развития информационно-технологической среды Боброва А.А.

Начальник управления Е.Н. Поздерин

УТВЕРЖДЕНО
приказом управления информационных технологий и связи Алтайского края
от 07.07 2016 № 55

ПОЛОЖЕНИЕ
об удостоверяющем центре Алтайского края

1. Общие положения

1.1. Удостоверяющий центр Алтайского края (далее – «удостоверяющий центр») создан в целях обеспечения органов исполнительной власти и органов местного самоуправления Алтайского края, а также подведомственных им учреждений квалифицированными электронными подписями для осуществления межведомственного электронного взаимодействия, оказания государственных и муниципальных услуг в электронном виде и иных функций, связанных с использованием электронной подписи.

1.2. Настоящее Положение определяет статус, цели, функции, структуру, порядок организации деятельности удостоверяющего центра, а также меры по обеспечению его информационной безопасности.

1.3. Удостоверяющий центр осуществляет свои функции в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, распоряжением Администрации Алтайского края от 08.06.2016 № 165-р, регламентом оказания услуг удостоверяющего центра и настоящим Положением.

1.4. Удостоверяющий центр ведет свою деятельность на основании лицензии УФСБ России по Алтайскому краю на право осуществления разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для собственных нужд юридического лица или индивидуального предпринимателя).

1.5. Удостоверяющий центр аккредитован уполномоченным федеральным органом исполнительной власти в сфере использования электронной подписи.

1.6. Удостоверяющий центр обеспечивает возможность по запросу за-

явителя включать в состав квалифицированного сертификата ключа проверки электронной подписи (далее – КСКПЭП) дополнительные ограничения использования в том случае, если сфера применения данного КСКПЭП ограничивается использованием в государственных информационных системах, либо информационных системах, по которым удостоверяющему центру предоставлено право выдавать КСКПЭП, содержащие соответствующие ограничения.

1.7. Порядок осуществления функций удостоверяющего центра, а также права, обязанности и ответственность, возникающие при выполнении им своей деятельности, определяются регламентом оказания услуг удостоверяющего центра, утвержденным начальником управления информационных технологий и связи Алтайского края (далее – «начальник Управления»).

2. Функции удостоверяющего центра

2.1. Удостоверяющий центр осуществляет следующие функции:

создание и выдача КСКПЭП, в том числе установление сроков действия КСКПЭП;

прекращение действия и аннулирование выданных удостоверяющим центром КСКПЭП;

ведение реестра выданных и аннулированных удостоверяющим центром КСКПЭП, в том числе включающего в себя информацию, содержащуюся в выданных удостоверяющим центром КСКПЭП, и информацию о датах прекращения действия или аннулирования КСКПЭП и о причинах прекращения или аннулирования;

создание ключей электронных подписей и ключей проверки электронных подписей;

проверка уникальности ключей проверки электронных подписей в реестре сертификатов;

осуществление проверки электронных подписей;

осуществление иной связанной с использованием электронной подписи деятельности.

3. Структура и порядок организации деятельности удостоверяющего центра

3.1. Удостоверяющий центр представляет собой совокупность программных и аппаратных средств, коммуникаций, средств защиты информации, помещения, аттестованного по требованиям безопасности информации, и персонала.

3.2. Обеспечение функционирования удостоверяющего центра возложено на отдел информационной безопасности в соответствии с положением об отделе и должностными регламентами сотрудников отдела, утвержденными начальником Управления.

3.3. Руководство деятельностью удостоверяющего центра и распределение обязанностей между сотрудниками отдела информационной безопас-

ности осуществляет начальник отдела информационной безопасности.

3.4. Начальник отдела несет персональную ответственность за выполнение функций, возложенных на удостоверяющий центр.

4. Обеспечение информационной безопасности удостоверяющего центра

4.1. Удостоверяющий центр обрабатывает информацию ограниченного доступа (в том числе персональные данные), не содержащую сведений, составляющих государственную тайну (далее – «информация конфиденциального характера»).

4.2. Безопасное функционирование удостоверяющего центра обеспечивается применением организационных и технических мер защиты, направленных на 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 конфиденциального характера, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением защищенности информации конфиденциального характера.