Ленинградское областное государственное автономное учреждение
«Кингисеппский центр социального обслуживания
граждан пожилого возраста и инвалидов»
(ЛОГАУ «Кингисеппский ЦСО»)

П Р И К А З

от 12.09.2024г. № 100

Об обеспечения информационной безопасности и осуществления мер, исключающих несанкционированный доступ к информационным ресурсам ЛОГАУ «Кингисеппский ЦСО»

В соответствии с Федеральными законами Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности», от 06.03.2006 № 35-ФЗ «О противодействии терроризму», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Ленинградской области от 11.09.2015 № 358 «Об утверждении типовых организационно-распорядительных документов операторов персональных данных», постановлением Правительства Российской Федерации от 13.05.2016 № 410 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства труда и социальной защиты Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, и формы паспорта безопасности этих объектов (территорий)», распоряжением комитета по социальной защите населения Ленинградской области от 03.05.2024 № 03-309, в целях выполнения требований безопасности и антитеррористической защищенности ЛОГАУ «Кингисеппский ЦСО»,обеспечения информационной безопасности и осуществления мер, исключающих несанкционированный доступ к информационным ресурсам

приказываю:

1. Назначить системного администратора Улитина А.И. ответственным за выполнение мероприятий по обеспечению информационной безопасности и осуществления мер, исключающих несанкционированный доступ к информационным ресурсам ЛОГАУ «Кингисеппский ЦСО».

2.В случае отсутствия системного администратора Улитина А.И. (командировка, отпуск, временная нетрудоспособность) ответственным за

выполнение мероприятий по обеспечению информационной безопасности и осуществления мер, исключающих несанкционированный доступ к информационным ресурсам ЛОГАУ «Кингисеппский ЦСО» назначить заместителя директора Иванову Н.С.

3. Утвердить типовые организационно-распорядительные документы ЛОГАУ «Кингисеппский ЦСО», являющиеся оператором персональных данных (приложение № 1).

4. Заместителю директора Ковалевской Ю.Н.в срок до 15 сентября 2024года ознакомить должностных лиц, указанных в пунктах 1,2 приказа под роспись.

5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Ю.М.Андреева

С приказом ознакомлены:

Ковалевская Ю.Н. «12» сентября»2024г.

Иванова Н.С. «12» сентября»2024г.

Улитин А.И. «12» сентября»2024г.

Утверждено
Приказом ЛОГАУ «Кингисеппский ЦСО»
от «12» сентября 2024 года № 100
(приложение №1)

ТИПОВЫЕ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ ЛОГАУ «Кингисеппский ЦСО», ЯВЛЯЮЩЕГОСЯ ОПЕРАТОРОМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1) Правила обработки персональных данных в ЛОГАУ «Кингисеппский ЦСО»;
2) Правила рассмотрения запросов субъектов персональных данных или их представителей в ЛОГАУ «Кингисеппский ЦСО»;
3) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами в ЛОГАУ «Кингисеппский ЦСО»;
4) Правила работы с обезличенными данными в случае обезличивания персональных данных в ЛОГАУ «Кингисеппский ЦСО»;
5) Перечень информационных систем персональных данных ЛОГАУ «Кингисеппский ЦСО»;
6) Перечень персональных данных, обрабатываемых в ЛОГАУ «Кингисеппский ЦСО» в связи с реализацией служебных или трудовых отношений, а также оказанием государственных услуг и осуществлением государственных функций;
7) Перечень должностей работников ЛОГАУ «Кингисеппский ЦСО», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
8) Перечень должностей работников ЛОГАУ «Кингисеппский ЦСО», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
9) Типовое обязательство работника ЛОГАУ «Кингисеппский ЦСО», непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;
10) Типовая форма согласия на обработку персональных данных субъектов персональных данных, а также разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
11) Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
12) Типовая форма согласия работника ЛОГАУ «Кингисеппский ЦСО» на доступ к информации ограниченного доступа;
13) Типовая форма обязательства о неразглашении информации, содержащей персональные данные, в ЛОГАУ «Кингисеппский ЦСО»;
14) Форма листа ознакомления работника ЛОГАУ «Кингисеппский ЦСО», непосредственно осуществляющего обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных);
15) Порядок доступа работников ЛОГАУ «Кингисеппский ЦСО» в помещения, в которых ведется обработка персональных данных;
16) Порядок доступа в помещения, где размещены используемые средства криптографический защиты информации, хранятся средства криптографический защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографический защиты информации, в рабочее и нерабочее время, а также в нештатных ситуациях в ЛОГАУ «Кингисеппский ЦСО»;
17) Типовой план правовых, организационных и технических мер по обеспечению безопасности персональных данных в ЛОГАУ «Кингисеппский ЦСО»;

18) Порядок проведения проверок соответствия обработки персональных данных установленным требованиям в ЛОГАУ «Кингисеппский ЦСО»;

19) Перечень должностей работников ЛОГАУ «Кингисеппский ЦСО», замещение которых предусматривает использование средств криптографической защиты информации;

20) Форма заключения о возможности эксплуатации средств криптографической защиты информации в ЛОГАУ «Кингисеппский ЦСО»;

21) Инструкция ответственного за эксплуатацию средств криптографической защиты информации в ЛОГАУ «Кингисеппский ЦСО»;

22) Инструкция пользователя средствами криптографической защиты информации в ЛОГАУ «Кингисеппский ЦСО»;

23) Инструкция по организации парольной защиты в ЛОГАУ «Кингисеппский ЦСО»;

24) Памятка пользователю средств криптографической защиты информации ЛОГАУ «Кингисеппский ЦСО;

25) Форма журнала поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов в ЛОГАУ «Кингисеппский ЦСО»;

26) Форма журнала учета выдачи машинных носителей в ЛОГАУ «Кингисеппский ЦСО»;

27) Форма журнала учета работников ЛОГАУ «Кингисеппский ЦСО», допущенных к работе со средствами криптографической защиты информации (СКЗИ);

28) Форма журнала ознакомления работников ЛОГАУ «Кингисеппский ЦСО» с нормативной документацией в области безопасности персональных данных;

29) Форма журнала учета мероприятий по контролю за соблюдением требований по обработке информации ограниченного доступа (персональных данных);

30) Форма журнала учета сейфов, металлических шкафов, специальных хранилищ и ключей от них.

ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
в ЛОГАУ «Кингисеппский ЦСО»

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
2. Обработка персональных данных в ЛОГАУ «Кингисеппский ЦСО» должна ограничиваться достижением конкретных заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
3.В ЛОГАУ «Кингисеппский ЦСО» не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.
7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
8. Мерами, направленными на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, являются:
1) назначение ответственного за организацию обработки персональных данных;
2) издание документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных;
3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
4) осуществление внутреннего контроля и(или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике ЛОГАУ «Кингисеппский ЦСО» в отношении обработки персональных данных, локальным актам ЛОГАУ «Кингисеппский ЦСО»;
5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
6) выполнение мероприятий по удалению или уточнению неполных или неточных данных;
7) ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ЛОГАУ «Кингисеппский ЦСО» в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и(или) обучение указанных работников.
9. Обеспечение безопасности персональных данных достигается:
1) определением угроз безопасности персональных данных;
2) применением организационных и(или) технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых

обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных, а также при обработке персональных данных без использования средств автоматизации;
3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
5) учетом машинных носителей персональных данных;
6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных, а также правил доступа к персональным данным при их обработке без использования средств автоматизации;
9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных, а также безопасности персональных данных, обрабатываемых без использования средств автоматизации.
10. Цели обработки персональных данных в ЛОГАУ «Кингисеппский ЦСО» определяются с учетом полномочий и функций ЛОГАУ «Кингисеппский ЦСО», определенных Уставом.
К персональным данным, обрабатываемым в указанных целях, относятся: фамилия, имя, отчество, пол, гражданство и т.д.
Обработка персональных данных в соответствии с указанными целями осуществляется в отношении субъектов персональных данных, являющихся работниками ЛОГАУ «Кингисеппский ЦСО», и(или) субъектов персональных данных, не являющихся сотрудниками ЛОГАУ «Кингисеппский ЦСО».
11. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных неправомерно обрабатываемые персональные данные, относящиеся к этому субъекту персональных данных, блокируются с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных персональные данные, относящиеся к этому субъекту персональных данных, блокируются с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.
12. В случае подтверждения факта неточности персональных данных ЛОГАУ «Кингисеппский ЦСО» на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.
13. В случае выявления неправомерной обработки персональных данных в срок, не превышающий трех рабочих дней с даты выявления, неправомерная обработка персональных данных прекращается. В случае если обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, такие персональные данные уничтожаются. Об устранении допущенных нарушений или об уничтожении персональных данных ЛОГАУ «Кингисеппский ЦСО» уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

14. В случае достижения цели обработки персональных данных обработка персональных данных прекращается и осуществляется их уничтожение в срок, не превышающий 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между ЛОГАУ «Кингисеппский ЦСО» и субъектом персональных данных либо если ЛОГАУ «Кингисеппский ЦСО»не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

15. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных обработка персональных данных прекращается и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, персональные данные уничтожаются в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между ЛОГАУ «Кингисеппский ЦСО» и субъектом персональных данных либо если ЛОГАУ «Кингисеппский ЦСО»не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

16. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 13 - 15 настоящих Правил, осуществляется блокирование таких персональных данных и уничтожение в срок не более шести месяцев, если иной срок не установлен федеральными законами.

ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ в ЛОГАУ «Кингисеппский ЦСО»

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
1) подтверждение факта обработки персональных данных;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые способы обработки персональных данных;
4) наименование и место нахождения ЛОГАУ «Кингисеппский ЦСО», сведения о лицах (за исключением работников ЛОГАУ «Кингисеппский ЦСО», которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ЛОГАУ «Кингисеппский ЦСО» или на основании федерального закона);
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;
8) информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению ЛОГАУ «Кингисеппский ЦСО», если обработка поручена или будет поручена такому лицу;
10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.
2. Субъект персональных данных вправе требовать от ЛОГАУ «Кингисеппский ЦСО»уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
3. Сведения предоставляются субъекту персональных данных ЛОГАУ «Кингисеппский ЦСО» в доступной форме без содержания персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
4. Сведения предоставляются субъекту персональных данных или его представителю ЛОГАУ «Кингисеппский ЦСО» при обращении либо при получении запроса субъекта персональных данных или его представителя.
Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с ЛОГАУ «Кингисеппский ЦСО» (номер договора, дата заключения договора, условное словесное обозначение и(или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных ЛОГАУ «Кингисеппский ЦСО», подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в ЛОГАУ «Кингисеппский ЦСО» или направить повторный запрос в целях ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно в ЛОГАУ «Кингисеппский ЦСО» или направить повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих Правил, должен содержать обоснование направления повторного запроса.

7. ЛОГАУ «Кингисеппский ЦСО» вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса возлагается на ЛОГАУ «Кингисеппский ЦСО».

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27.07.2006 № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ», ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ АКТАМИ ЛОГАУ «Кингисеппский ЦСО»

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в ЛОГАУ «Кингисеппский ЦСО» организуется проведение периодических проверок условий обработки персональных данных.
2. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в ЛОГАУ «Кингисеппский ЦСО», либо комиссией, образуемой приказом руководителя ЛОГАУ «Кингисеппский ЦСО».
3. В проведении проверки не может участвовать должностное лицо, прямо или косвенно заинтересованное в ее результатах.
4. Проверки соответствия обработки персональных данных установленным требованиям проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в ЛОГАУ «Кингисеппский ЦСО»письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.
5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне определены:
1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
2) порядок и условия применения средств защиты информации;
3) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
4) состояние учета машинных носителей персональных данных;
5) соблюдение правил доступа к персональным данным;
6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
7) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8) мероприятия по обеспечению целостности персональных данных.
6. Должностное лицо, ответственное за организацию обработки персональных данных (комиссия), имеет право:
1) запрашивать у должностных лиц ЛОГАУ «Кингисеппский ЦСО» информацию, необходимую для исполнения своих обязанностей;
2) требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
3) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
4) представлять руководителю ЛОГАУ «Кингисеппский ЦСО» предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
5) представлять руководителю ЛОГАУ «Кингисеппский ЦСО» предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в части обработки персональных данных.
7. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных (комиссии) в ходе проведения мероприятий внутреннего

контроля, должна обеспечиваться конфиденциальность персональных данных.

8. Проверка должна быть завершена не позднее чем через десять дней со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю ЛОГАУ «Кингисеппский ЦСО» докладывает должностное лицо, ответственное за организацию обработки персональных данных, либо председатель комиссии в форме письменного заключения.

ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ В СЛУЧАЕ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ВЛОГАУ «Кингисеппский ЦСО»

1. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
2. Методы обезличивания при условии дальнейшей обработки персональных данных:
1) метод введения идентификаторов - замена части значений персональных данных (далее - сведения) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;
2) метод изменения состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений (понижение точности некоторых сведений). Например, данные о месте жительства могут включать страну, индекс, город, улицу, номер дома и квартиры, а может быть указан только город;
3) метод декомпозиции - деление сведений на части с последующим раздельным хранением и обработкой в разных информационных системах;
4) метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).
3. Решение о необходимости обезличивания персональных данных принимает руководитель ЛОГАУ «Кингисеппский ЦСО».
4. Руководители структурных подразделений ЛОГАУ «Кингисеппский ЦСО», в которых осуществляется обработка персональных данных, подготавливают предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.
5. Должностные лица ЛОГАУ «Кингисеппский ЦСО», обслуживающие базы персональных данных, совместно с должностным лицом, ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.
6. Обезличенные персональные данные не подлежат разглашению и нарушению их конфиденциальности.
7. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.
8. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:
1) парольной политики, регламентирующей требования к сложности и частоте изменения паролей, к действиям пользователей при работе с паролями;
2) антивирусной политики, устанавливающей требования к пользователям и администраторам по настройке и использованию средств антивирусной защиты;
3) правил работы со съемными носителями (если они используются);
4) правил резервного копирования;
5) правил доступа в помещения, где расположены элементы информационных систем.
9. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
1) правил хранения бумажных носителей;
2) правил доступа к бумажным носителям и в помещения, где они хранятся.

ПЕРЕЧЕНЬ
ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛОГАУ «Кингисеппский ЦСО»

Наименование ИСПДн (ее сегмента)	Наименование объекта (полное и сокращенное). Отраслевая принадлежность. Адрес объекта	Структура ИСПДн	Наличие подключений к информационно-телекоммуникационным сетям международного информационного обмена (Интернет)	Режим обработки персональных данных	Нахождение ИСПДн (ее составных частей) в пределах Российской Федерации	Категории персональных данных, субъекты, в отношении которых ведется обработка	Уровень защищенности ИСПДн
Государственная информационная система Ленинградской области «Управление бюджетным процессом Ленинградской области»	Комитет финансов Ленинградской области; отрасль – финансовый орган исполнительной власти 191311, г. Санкт-Петербург ,Суворовский проспект, д.67	Распределенная информационная система	Присутствует	Многопользовательский с различными правами доступа	Все технические средства находятся на территории Российской Федерации	ПДн субъектов, являющихся сотрудниками ЛОГАУ «Кингисеппский ЦСО»	2
Государственная информационная система Ленинградской области «Автоматизированная информационная система «Социальная защита Ленинградской области»	Комитет по социальной защите населения Ленинградской области; отрасль – социальное обеспечение. 191124, г. Санкт-Петербург , ул. Лафонская, д. 6, литер а	Распределенная информационная система	Присутствует	Многопользовательский с различными правами доступа	Все технические средства находятся на территории Российской Федерации	ПДн субъектов, не являющихся сотрудниками ЛОГАУ «Кингисеппский ЦСО»	2

ПЕРЕЧЕНЬ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ
В ЛОГАУ «Кингисеппский ЦСО»
В СВЯЗИ С РЕАЛИЗАЦИЕЙ СЛУЖЕБНЫХ ИЛИ ТРУДОВЫХ ОТНОШЕНИЙ,
А ТАКЖЕ ОКАЗАНИЕМ ГОСУДАРСТВЕННЫХ УСЛУГ И ОСУЩЕСТВЛЕНИЕМ ГОСУДАРСТВЕННЫХ ФУНКЦИЙ

фамилия, имя, отчество
информация о смене фамилии, имени, отчества
пол
дата рождения
место рождения
гражданство
документ, удостоверяющий личность (серия, номер, когда и кем выдан)
сведения из записей актов гражданского состояния
место жительства и дата регистрации по месту жительства
номера контактных телефонов
семейное положение
состав семьи
сведения о наличии детей, их возрасте, месте учебы (работы)
сведения, содержащиеся в служебном контракте, трудовом договоре
отношение к воинской обязанности, воинское звание, состав рода войск, военный билет, приписное свидетельство, сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах

сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, квалификации, наименование документа об образовании, его серия и номер, дата выдачи)
сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка)
сведения о профессиональной переподготовке, повышении квалификации, стажировке
сведения о трудовой деятельности, общем трудовом стаже и стаже государственной гражданской службы
сведения о замещаемой должности
сведения о классных чинах, военных и специальных званиях
сведения о состоянии здоровья и его соответствии выполняемой работе, наличии группы инвалидности и степени ограничения способности к трудовой деятельности
сведения об отпусках и командировках
сведения о прохождении аттестации и сдаче квалификационного экзамена
сведения о документах, связанных с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности связано с использованием таких сведений
сведения о награждении (поощрении)
материалы служебных проверок, расследований
сведения о взысканиях
реквизиты идентификационного номера налогоплательщика (ИНН)
реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС)
реквизиты полиса обязательного медицинского страхования
сведения о доходах, имуществе и обязательствах имущественного характера государственного гражданского служащего и членов его семьи

сведения о социальных льготах
информация о доходах, выплатах и удержаниях
номера банковских счетов
фото
Персональные данные, обрабатываемые в ЛОГАУ «Кингисеппский ЦСО» в связи с оказанием государственных услуг и осуществлением государственных функций:
фамилия, имя, отчество
пол
дата рождения
место рождения
документ, удостоверяющий личность (серия, номер, когда и кем выдан)
адрес регистрации, фактического проживания
контактный номер телефона
данные о состоянии здоровья (история болезни)
группа инвалидности
иные персональные данные, необходимые для оказания социальной помощи
Персональные данные граждан, обрабатываемые в связи с рассмотрением обращений граждан:
фамилия, имя, отчество
адрес места жительства
иные персональные данные, содержащиеся в обращениях граждан

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ РАБОТНИКОВЛОГАУ «Кингисеппский ЦСО», ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наименование должности ответственного лица	Документ о назначении ответственного лица
----------	----------

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ РАБОТНИКОВЛОГАУ «Кингисеппский ЦСО», ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

Наименование должности	**Подразделение**	**Документ, предусматривающий осуществление обработки персональных данных должностным лицом либо доступ к персональным данным в ЛОГАУ «Кингисеппский ЦСО»**
Специалист по кадрам	Административно - хозяйственная часть	Должностная инструкция
Главный бухгалтер	Административно - хозяйственная часть	Должностная инструкция
Бухгалтер	Административно - хозяйственная часть	Должностная инструкция
Заведующие отделениями	Реабилитационное отделение социального обслуживания Отделения социальной помощи на дому	Должностная инструкция
Специалисты, работающие в АИС «Соцзащита»	Реабилитационное отделение социального обслуживания Отделения социальной помощи на дому	Приказ по учреждению

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
РАБОТНИКА ЛОГАУ «Кингисеппский ЦСО», НЕПОСРЕДСТВЕННО ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, В СЛУЧАЕ РАСТОРЖЕНИЯ С НИМ ТРУДОВОГО ДОГОВОРА ПРЕКРАТИТЬ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, СТАВШИХ ИЗВЕСТНЫМИ ЕМУ В СВЯЗИ С ИСПОЛНЕНИЕМ ДОЛЖНОСТНЫХ ОБЯЗАННОСТЕЙ

Я,_____,
(фамилия, имя, отчество полностью)

_____
(наименование должности и структурного подразделения)

_____

_____

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____ _____
(дата) (подпись) (фамилия, инициалы)

ТИПОВАЯ ФОРМА СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ РАЗЪЯСНЕНИЯ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЙ ОТКАЗА ПРЕДОСТАВИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я, _____,
(фамилия, имя, отчество полностью)

_____
(вид документа, удостоверяющего личность, серия, номер, когда и кем выдан,

_____
реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

настоящим даю согласие на обработку в «____» моих персональных данных (персональных данных представляемого) и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах (в интересах представляемого).

Согласие дается мною для: обеспечения соблюдения законов и иных нормативных правовых актов в сфере обработки персональных данных и осуществления полномочий «____»в части оператора данных.
(цель (цели) обработки персональных данных)

Настоящее согласие предоставляется на осуществление любых действий по обработке моих персональных данных (персональных данных представляемого) для достижения указанных целей в соответствии с требованиями, установленными Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, и действует со дня его подписания и до достижения целей обработки персональных данных, указанных в данном согласии, либо до дня отзыва согласия на обработку персональных данных в письменной форме.

_____ _____ _____
(дата) (подпись) (фамилия, инициалы)

Предоставленные данные соответствуют предъявленным документам, удостоверяющим личность.

_____ _____ _____
(дата) (подпись) (фамилия, инициалы должностного лица, принявшего документ)

РАЗЪЯСНЕНИЕ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЙ ОТКАЗА ПРЕДОСТАВИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ
(для работников)

Мне, _____,
(фамилия, имя, отчество полностью)
разъяснены юридические последствия отказа предоставить свои персональные данные: _____.
(указать)

В соответствии со статьями 57, 65, 69 Трудового кодекса Российской Федерации субъект персональных данных - лицо, поступающее на работу или работающее, обязано предоставить информацию о себе.

Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений трудовой договор не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

_____ _____ _____
(дата) (подпись) (фамилия, инициалы)

ТИПОВАЯ ФОРМА
СОГЛАСИЯ РАБОТНИКА ЛОГАУ «Кингисеппский ЦСО» НА ДОСТУП К ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Я,_____,
(фамилия, имя, отчество полностью)
зарегистрированный (-ая) по адресу: _____
_____
(индекс и адрес регистрации согласно паспорту)
_____
_____
Паспорт серия _____ № _____ выдан _____
_____
(наименование органа, выдавшего паспорт, и дата выдачи)
являясь работником «____», находящегося по адресу:_____, своей волей и в своем интересе выражаю согласие на получение доступа к информации ограниченного доступа, в соответствии с функциональными обязанностями, возложенными на меня, но не предусмотренных моим служебным контрактом.

В соответствии с законодательством Российской Федерации обязуюсь не разглашать сведения о персональных данных сотрудников «____», и иные сведения (информацию) ограниченного доступа, ставших известными мне в связи с исполнением трудовых обязанностей.

С «Правилами обработки персональных данных в «____» и ответственностью за неисполнение или ненадлежащее исполнение этого согласия ознакомлен.

Настоящее согласие вступает в силу с момента его подписания на срок действия трудового договора и в течение трех лет после его прекращения.

_____ _____ _____
(дата) (подпись) (фамилия, инициалы)

ТИПОВАЯ ФОРМА ОБЯЗАТЕЛЬСТВА О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, в ЛОГАУ «Кингисеппский ЦСО»

Я,_____,
(фамилия, имя, отчество полностью)
исполняющий (ая) должностные обязанности по замещаемой должности _____
_____
___
_____
__ ,
(должность, наименование структурного подразделения)
предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ _____ _____
(дата) (подпись) (фамилия, инициалы)

ФОРМА ЛИСТА ОЗНАКОМЛЕНИЯ РАБОТНИКА ЛОГАУ «Кингисеппский ЦСО», НЕПОСРЕДСТВЕННО ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, С ПОЛОЖЕНИЯМИ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ О ПЕРСОНАЛЬНЫХ ДАННЫХ (В ТОМ ЧИСЛЕ С ТРЕБОВАНИЯМИ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ)

Я,_____,

(фамилия, имя, отчество полностью)

_____

_____ ,

(должность, наименование структурного подразделения)

ознакомлен(а) с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), правовыми актами по вопросам обработки персональных данных.

Мною изучены положения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и правовые акты ЛОГАУ «Кингисеппский ЦСО», определяющие политику в отношении обработки персональных данных.

Я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известных мне в связи с исполнением должностных обязанностей.

Ответственность и права, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснены.

_____ _____ _____

(дата) (подпись) (фамилия, инициалы)

ПОРЯДОК
ДОСТУПА РАБОТНИКОВ ЛОГАУ «Кингисеппский ЦСО» В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Персональные данные относятся к категории конфиденциальной информации. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
2. Перечень должностей работников ЛОГАУ «Кингисеппский ЦСО», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным утверждается руководителем ЛОГАУ «Кингисеппский ЦСО».
3. Порядок определяет правила доступа в помещения, где хранятся и обрабатываются персональные данные в целях исключения несанкционированного доступа к персональным данным, а также обеспечения безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий
в отношении персональных данных.
4. В помещения, где размещены материальные носители информации, содержащие персональные данные, допускаются только должностные лица ЛОГАУ «Кингисеппский ЦСО», имеющие доступ к персональным данным.
5. Должностные лица, имеющие доступ к персональным данным, не должны:
- оставлять в свое отсутствие незапертым помещение, в котором размещены технические средства, позволяющие осуществлять обработку персональных данных;
- оставлять в помещении посторонних лиц, не имеющих доступа к персональным данным в данном структурном подразделении, без присмотра.
6. Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащей персональные данные, а также исключается возможность неконтролируемого проникновения
и пребывания в этих помещениях посторонних лиц. Указанный режим обеспечивается в том числе:
- оснащением помещения охранной и пожарной сигнализацией;
- обязательным запиранием помещения на ключ при выходе из него даже в рабочее время;
- закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные.
7. Доступ в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся материальные носители персональных данных, в случае возникновения непредвиденных обстоятельств в нерабочее время осуществляется сотрудником службы безопасности с записью в журнале вскрытия.
8. Ответственность за соблюдение настоящего Порядка возлагается на заведующих отделов ЛОГАУ «Кингисеппский ЦСО», в которых ведется обработка персональных данных и осуществляется их хранение.
9. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных, или комиссией, образуемой руководителем ЛОГАУ «Кингисеппский ЦСО».

ПОРЯДОК
ДОСТУПА В ПОМЕЩЕНИЯ, ГДЕ РАЗМЕЩЕНЫ ИСПОЛЬЗУЕМЫЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ХРАНЯТСЯ СРЕДСТВА КРИПТОГРАФИЧЕСКИЙ ЗАЩИТЫ ИНФОРМАЦИИ И (ИЛИ) НОСИТЕЛИ КЛЮЧЕВОЙ, АУТЕНТИФИЦИРУЮЩЕЙ И ПАРОЛЬНОЙ ИНФОРМАЦИИ СРЕДСТВ КРИПТОГРАФИЧЕСКИЙ ЗАЩИТЫ ИНФОРМАЦИИ, В РАБОЧЕЕ И НЕРАБОЧЕЕ ВРЕМЯ, А ТАКЖЕ В НЕШТАТНЫХ СИТУАЦИЯХ В ЛОГАУ «Кингисеппский ЦСО»

Доступ в помещения, в которых ведется обработка конфиденциальной информации, в том числе персональных данных (далее – ПД), и где размещены используемые средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, осуществляется с учетом обеспечения безопасности ПД.

Для помещений ЛОГАУ «Кингисеппский ЦСО», в которых обрабатывается ПД и где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения), должен обеспечиваться режим безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

Право самостоятельного входа в помещения имеют работники ЛОГАУ «Кингисеппский ЦСО», непосредственно работающие в этих помещениях, лицо, ответственное за организацию работ по обработке ПД граждан в ЛОГАУ «Кингисеппский ЦСО», лицо, ответственное за защиту ПД граждан в ЛОГАУ «Кингисеппский ЦСО», и администратор безопасности информации на объектах.

Иные лица допускаются в Помещения по согласованию с непосредственным руководителем или его заместителем по направлению деятельности и в сопровождении лица, работающего в этом Помещении.

Помещения по окончании рабочего дня должны закрываться на ключ.

Вскрытие и закрытие Помещения производится лицами, имеющими право доступа.

Уборка Помещения должна производиться в присутствии лица, допущенного к осуществлению обработки ПД.

Перед закрытием Помещения по окончании рабочего дня, лица, имеющие право доступа в помещения, обязаны:

- убрать материальные носители ПД в шкафы, закрыть и опечатать шкафы;
- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;
- закрыть окна.

Перед открытием Помещения лица, имеющие право доступа в помещения, обязаны:

- провести внешний осмотр с целью установления целостности двери;
- открыть дверь и осмотреть Помещение, проверить наличие и целостность печатей на шкафах, где хранятся материальные носители.

При обнаружении неисправности двери и запирающих устройств необходимо:

- не вскрывая Помещение, доложить непосредственному руководителю;

в присутствии лица, ответственного за организацию работ по обработке ПД граждан в ЛОГАУ «Кингисеппский ЦСО», либо лица, ответственного за защиту ПД граждан в ЛОГАУ «Кингисеппский ЦСО», либо администратора безопасности информации на объектах и непосредственного руководителя, вскрыть Помещение и осмотреть его;

- составить акт о выявленных нарушениях и передать его руководителю ЛОГАУ «Кингисеппский ЦСО» для организации служебного расследования.

Ответственность за соблюдение порядка доступа в Помещения возлагается на лиц, обрабатывающих ПД.

В Помещениях, в которых размещаются информационные системы персональных данных и где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, необходимо обеспечение режима безопасности, который достигается путем оснащения таких помещений входными дверьми с замками, обеспечения постоянного закрытия дверей на замок и их открытия только для санкционированного прохода, а также опечатывания их по окончании рабочего дня или оборудование таких помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии.

Помещения располагаются в пределах контролируемой зоны, границами которой являются ограждающие конструкции зданий, в которых они размещены, с учётом территорий, контролируемых службами охраны.

Вскрытие и закрытие (опечатывание) Помещений, производится должностными лицами, имеющими право доступа в данные помещения.

Должностные лица, имеющие право доступа в Помещения не должны:

- оставлять в свое отсутствие незапертым Помещение;
- оставлять в Помещении посторонних лиц, не имеющих право доступа в такое помещение, без присмотра.

Обслуживание и сопровождение технических и программных средств, уборка, проведение других работ в Помещениях осуществляются в присутствии должностного лица, имеющего право доступа в данное помещение.

В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка защищаемой информации, в нерабочее время, вскрытие Помещения осуществляется сторожем (вахтером) непосредственно находящимся на дежурстве, который ставит в известность ответственного за организацию работ по обработке ПД граждан в ЛОГАУ «Кингисеппский ЦСО» , либо лицо, ответственное за защиту ПД граждан в ЛОГАУ «Кингисеппский ЦСО», либо администратора безопасности информации на объектах, а так же лиц, имеющих право допуска в данное помещение, в начале следующего рабочего дня.

Ответственность за соблюдение настоящего порядка возлагается на заместителя директора, курирующего данное направление работы.

ТИПОВОЙ ПЛАН
ПРАВОВЫХ, ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ВЛОГАУ «Кингисеппский ЦСО»

№ п/п	Наименование мероприятия	Исполнитель	Сроки выполнения	Отметка о выполнении
1	2	3	4	5
1	Аудит соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»			
2	Издание необходимой или актуализация имеющейся организационно-распорядительной документации, определяющей правила обработки персональных данных, а также устанавливающей процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации о персональных данных, устранение последствий таких нарушений			
3	Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»			
4	Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, локальными актами по вопросам обработки персональных данных			
5	Повышение квалификации (переподготовка) ответственного за обработку персональных данных по вопросам, связанным с исполнением возложенных на него должностных обязанностей			
6	Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и при необходимости формирование требований к их защите			
	Оценка эффективности принимаемых мер по обеспечению			

7	безопасности персональных данных			
8	Проведение внутреннего контроля соответствия организации и состояния работ по выполнению ЛОГАУ «Кингисеппский ЦСО» обязательств в отношении обработки персональных данных, в том числе обеспечению безопасности персональных данных, требованиям локальных актов ЛОГАУ «Кингисеппский ЦСО», законодательства Российской Федерации о персональных данных			
9	Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных			

Ответственный за организацию
обработки персональных данных _____ _____
(подпись) (фамилия, инициалы)

ПОРЯДОК
ПРОВЕДЕНИЯ ПРОВЕРОК СООТВЕТСТВИЯ ОБРАБОТКИ
ПЕРСОНАЛЬНЫХ ДАННЫХ УСТАНОВЛЕННЫМ ТРЕБОВАНИЯМ
В ЛОГАУ «Кингисеппский ЦСО»

№ п/п	Краткое описание мероприятий	Периодичность мероприятий	Результат проверки	Фамилия, имя, отчество ответственного пользователя, подпись	Фамилия, имя, отчество лица, проводившего проверку, подпись	Примечание
1	2	3	4	5	6	7
1	Контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны	Не реже одного раза в три года или при необходимости				
2	Проверка выполнения требований по условиям размещения автоматизированных рабочих мест (далее - АРМ) в помещениях, в которых размещены средства информационных систем персональных данных (далее - ИСПДн)	Не реже одного раза в год или в зависимости от изменения расположения АРМ или ИСПДн				
3	Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, разрешенных для обработки персональных данных	Не реже одного раза в год или в зависимости от изменения состава и структуры таких средств				
4	Проверка режима допуска в помещения, где размещены средства ИСПДн и осуществляется обработка персональных	Не реже одного раза в год				

	данных					
5	Проверка соответствия реального уровня полномочий по доступу к персональным данным различных пользователей, установленному в списке лиц, допущенных к обработке персональных данных, уровню полномочий	Не реже одного раза в год				
6	Проверка наличия и соответствия средств защиты информации в соответствии с указанными в техническом паспорте на ИСПДн	Не реже одного раза в год				
7	Проверка правильности применения средств защиты информации	При необходимости				
8	Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей	Не реже одного раза в год				
9	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн	В зависимости от частоты обновления программного обеспечения				
10	Проверка соблюдения правил парольной защиты	Не реже одного раза в год				
11	Проверка работоспособности системы резервного копирования	Не реже одного раза в год				
12	Проведение мероприятий по проверке организации учета	Не реже одного раза в год				

	и условий хранения съемных носителей персональных данных					
13	Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети «Интернет»	Не реже одного раза в год				
14	Проверка знаний работниками руководящих документов, технологических инструкций, предписаний, актов, заключений и уровня овладения работниками технологией безопасной обработки информации, изложенных в инструкциях	Не реже одного раза в год				
15	Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн	Не реже одного раза в год				
16	Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки персональных данных и применения средств защиты (сертификатов соответствия и других документов)	Не реже одного раза в год				

Ответственный за организацию
обработки персональных данных _____ _____
(подпись) (фамилия, инициалы)

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ СЛУЖАЩИХ (СОТРУДНИКОВ) ЛОГАУ «Кингисеппский ЦСО», ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ИСПОЛЬЗОВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Наименование должности	**Подразделение**
Специалист по кадрам	Административно -хозяйственная часть
Главный бухгалтер	Административно -хозяйственная часть
Бухгалтер	Административно -хозяйственная часть

ФОРМА ЗАКЛЮЧЕНИЯ О ВОЗМОЖНОСТИ ЭКСПЛУАТАЦИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ВЛОГАУ «Кингисеппский ЦСО»

Настоящее заключение составлено в том, что администратором безопасности «____»
_____
(фамилия, имя, отчество полностью)
назначенным приказом«____» от «__» _____ 20__ г. № _____,
в период с «__» _____ 20__ г. по «__» _____ 20__ г. в присутствии пользователя средств криптографической защиты информации (далее – СКЗИ)
_____
(должность, фамилия, имя, отчество полностью)
были проведены работы по установке, проверке работоспособности, соответствия условий и режимов эксплуатации СКЗИ, указанных в Таблице, требованиям эксплуатационной и технической документации к ним, а также Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации от 13.06.2001 № 152 (Инструкция № 152).

Таблица

п/п	Наименование / модель технического средства[1]	Заводской номер технического средства[1]	Тип (наименование) установленного СКЗИ	Заводской / регистрационный номер установленного СКЗИ	№ печати, которой опечатано техническое средство[1]	Место установки
1	2	3	4	5	6	7

Администратором безопасности в присутствии начальника отдела (сектора)
_____
(наименование структурного подразделения)
_____
(фамилия, имя, отчество полностью)
по результату сдачи пользователем СКЗИ зачета по программе_____
_____
(наименование программы)
была подтверждена должная специальная подготовка пользователя СКЗИ и возможность его допуска к самостоятельной работе с СКЗИ.

В результате выполнения указанных организационно-технических мероприятий нарушений требований Инструкции № 152, эксплуатационной и технической документации к СКЗИ не выявлено, принято решение о возможности эксплуатации СКЗИ, указанных в Таблице.

Заключение составлено в двух экземплярах. Один экземпляр подлежит хранению в деле №_____, второй – передаче в ГКУ ЛО «Оператор электронного правительства».

---

[1] Аппаратное, программное или аппаратно-программное средство, где установлены или к которым подключены СКЗИ

Администратор безопасности

_____ (Подпись)

_____ (Фамилия И.О.)

_____ (Дата)

Пользователь СКЗИ

_____ (Подпись)

_____ (Фамилия И.О.)

_____ (Дата)

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОГО ЗА ЭКСПЛУАТАЦИЮ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОГАУ «Кингисеппский ЦСО»

Общие положения

Все действия со средствами криптографической защитой информации (далее - СКЗИ) осуществляются в соответствии с эксплуатационной документацией на СКЗИ.

Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления сведениями об уникальной последовательности символов, предназначенных для создания СКЗИ (крипграфическими ключами), приказом ЛОГАУ «Кингисеппский ЦСО» назначается администратор безопасности информации на объектах (далее – ответственный в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ).

Ответственный за эксплуатацию СКЗИ в ЛОГАУ «Кингисеппский ЦСО» осуществляет:

поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;

- учет пользователей СКЗИ;
- обучение пользователей правилам эксплуатации СКЗИ;
- контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;
- разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на ответственного за эксплуатацию СКЗИ.

Ответственный за эксплуатацию СКЗИ должен быть ознакомлен с настоящей Инструкцией под расписку.

Учет и хранение СКЗИ и криптографических ключей

В ЛОГАУ «Кингисеппский ЦСО» СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

Поэкземплярный учет СКЗИ ведет ответственный за эксплуатацию СКЗИ в журнале поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним, ключевых документов в ЛОГАУ «Кингисеппский ЦСО» (далее – Журнал). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под расписку в журнале поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов в ЛОГАУ «Кингисеппский ЦСО», пользователям СКЗИ, несущим персональную ответственность за их сохранность.

Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у ответственного за эксплуатацию СКЗИ. Криптографические ключи хранятся у пользователей СКЗИ. Хранение осуществляется в закрываемых на замок металлических хранилищах пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение, или в опечатанном пенале (тубусе). Металлические шкафы должны быть оборудованы внутренними замками с двумя экземплярами ключей, кодовыми замками и приспособлениями для опечатывания. Один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию СКЗИ, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе.

На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие надписи: на один ключевой носитель - «Рабочий»; на другой ключевой носитель - «Резервный».

Ключевой носитель с наклейкой «Резервный» помещается в конверт и опечатывается пользователем и ответственным за эксплуатацию СКЗИ.

Все полученные экземпляры криптографических ключей должны быть выданы под расписку в Журнале. Резервные криптографические ключи могут находиться на хранении у ответственного за эксплуатацию СКЗИ.

Ключевые носители с неработоспособными криптографическими ключами ответственный за эксплуатацию СКЗИ принимает от пользователя под расписку в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

При необходимости замены наклейки на ключевом носителе (стирание надписи реквизитов) пользователь передает его ответственному за эксплуатацию СКЗИ, который в присутствии пользователя снимает старую наклейку и приклеивает новую наклейку с такими же учетными реквизитами.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

СКЗИ и криптографические ключи могут доставляться специальной (фельдъегерской) связью или курьером, имеющего доверенность, подписанную руководителем, на право получения СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

Для пересылки СКЗИ и криптографические ключи помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптографические ключи пересылают в отдельном пакете с пометкой «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения целостности упаковок и оттисков печати.

Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приема-передачи, в котором указывается: что посылается и в каком количестве, учетные номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приема-передачи документов вкладывается в упаковку.

Полученную упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приема-передачи документов или сама упаковка и оттиск печати - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то должен быть составлен Акт о происшедшем нарушении. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний от руководителя применять не разрешается.

При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует возвратить для установления причин происшедшего и их устранения в дальнейшем. В этом случае необходимо получить новые криптографические ключи.

Ключевые носители совместно с Журналом должны храниться ответственным в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.

На время отсутствия ответственного в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ его замещает ответственный за защиту персональных данных граждан в ЛОГАУ «Кингисеппский ЦСО».

При необходимости криптографические ключи сдаются на временное хранение ответственному в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ.

Использование СКЗИ и криптографических ключей

Криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

Криптографический ключ невозможно использовать, если истек срок действия.

Для обеспечения контроля доступа к СКЗИ системный блок персональной электронно-вычислительной машины (далее – ПЭВМ) опечатывается ответственным за эксплуатацию СКЗИ.

Пользователь должен периодически (ежедневно) проверять сохранность оборудования и целостность печатей на ПЭВМ. В случае обнаружения «посторонних» (не зарегистрированных) программ или выявления факта повреждения печати на системном блоке ПЭВМ работа должна быть прекращена. По данному факту проводится служебное расследование, и осуществляются работы по анализу и ликвидации последствий данного нарушения.

При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей ответственный в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ выполняет в присутствии пользователя.

В случае, если рабочие криптографические ключи потеряли работоспособность, то по просьбе пользователя ответственный в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ, вскрывает конверт (коробку) с резервными криптографическими ключами, делает копию ключевого носителя, используя резервные криптографические ключи, помещает резервные криптографические ключи в конверт (коробку), а на новый ключевой носитель наклеивает наклейку с надписью «Рабочий».

В экстренных случаях, не терпящих отлагательства, вскрытие конверта (коробки) с резервными криптографическими ключами может осуществляться комиссионно, с последующим уведомлением ответственного в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются ответственному в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ.

Вскрытие системного блока ПЭВМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ, либо ответственного за защиту персональных данных граждан в ЛОГАУ «Кингисеппский ЦСО».

Изготовление и плановая смена криптографических ключей

Изготовление криптографических ключей может производиться ответственным в ЛОГАУ «Кингисеппский ЦСО» за эксплуатацию СКЗИ в присутствии пользователя.

Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (электронный идентификатор) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

В целях обеспечения непрерывности проведения работы, плановую смену криптографических ключей следует производить заблаговременно, до окончания срока действия закрытых криптографических ключей.

При замене криптографических ключей используют программное обеспечение в соответствии с документацией по эксплуатации.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
ЛОГАУ «Кингисеппский ЦСО»

Пользователи средств криптографической защиты информации (далее - СКЗИ) обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, и сведения об уникальной последовательности символов, предназначенных для создания СКЗИ (криптоключах);
- соблюдать требования по обеспечению безопасности информации с использованием СКЗИ;
- сообщать администратору безопасности информации на объектах в ЛОГАУ «Кингисеппский ЦСО» о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах;
- сдать администратору безопасности информации на объектах в ЛОГАУ «Кингисеппский ЦСО» эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять администратора безопасности информации на объектах в ЛОГАУ «Кингисеппский ЦСО» о фактах утраты или недостачи СКЗИ, ключевых документов, ключей от помещений, сейфов, личных печатей.

Пользователи СКЗИ несут персональную ответственность за сохранность СКЗИ и ключевых документов.

Не допускается:

- производить несанкционированное копирование ключевых документов;
- знакомить или передавать ключевые документы лицам, к ним не допущенным;
- выводить ключевые документы на дисплей или принтер;
- вставлять носители ключевой информации в считывающие устройства других компьютеров;
- оставлять носители ключевой информации без присмотра на рабочем месте;
- записывать на носители ключевой информации посторонние файлы.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ ЛОГАУ «Кингисеппский ЦСО»

1. Общие положения

1.1 Настоящая инструкция устанавливает основные правила введения парольной защиты в ЛОГАУ «Кингисеппский ЦСО». Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в ЛОГАУ «Кингисеппский ЦСО», а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

Несанкционированный доступ – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Правила доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Пароль – уникальный признак субъекта доступа, который является его (субъекта) секретом.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

2. Правила генерации паролей

2.1 Персональные пароли должны генерироваться специальными программными средствами административной службы.

2.2 Длина пароля должна быть не менее 8 символов.

2.3 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.4 Пароль не должен включать в себя:

- легко вычисляемые сочетания символов;
- клавиатурные последовательности символов и знаков;
- общепринятые сокращения;
- аббревиатуры;
- номера телефонов, автомобилей;
- прочие сочетания букв и знаков, ассоциируемые с пользователем;
- при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

2.5 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам ЛОГАУ «Кингисеппский ЦСО».

3. Порядок смены паролей

3.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одно раза в месяц.

3.2 Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.

3.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ЛОГАУ «Кингисеппский ЦСО».

3.4 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4. Обязанности пользователей при работе с парольной защитой

4.1 При работе с парольной защитой пользователям запрещается:

- разглашать кому либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи и информации, хранящейся в ЛОГАУ «Кингисеппский ЦСО»посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

4.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

4.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5. Случаи компрометации паролей

5.1 Под компрометацией следует понимать:

- физическая утеря носителя с информацией;
- передача идентификационной информации по открытым каналам связи;
- проникновение постороннего лица в место физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

5.2 Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

6. Ответственность пользователей при работе с парольной защитой

6.1 Повседневный контроль за действиями работников ЛОГАУ «Кингисеппский ЦСО» при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на администратора безопасности информации на объектах в ЛОГАУ «Кингисеппский ЦСО».

6.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6.3 Ответственность за организацию парольной защиты возлагается на ответственного за защиту персональных данных граждан в ЛОГАУ «Кингисеппский ЦСО».

6.4 Ответственность в случае несвоевременного уведомления ответственного за защиту персональных данных граждан в ЛОГАУ «Кингисеппский ЦСО» о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

ПАМЯТКА ПОЛЬЗОВАТЕЛЮ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ЛОГАУ «Кингисеппский ЦСО»

При организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации (далее - СКЗИ) (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, обладатель и пользователь СКЗИ должен руководствоваться приказом Федеральное агентство правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (далее - Инструкция № 152).

Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.

Пользователи СКЗИ обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения об уникальной последовательности символов, предназначенных для создания СКЗИ (криптоключах);
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать администратору безопасности информации на объектах в ЛОГАУ «Кингисеппский ЦСО» или в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять администратора безопасности информации на объектах в ЛОГАУ «Кингисеппский ЦСО» или орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов в ЛОГАУ «Кингисеппский ЦСО» (далее – Журнал).

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих Журналах. Такая передача между пользователями СКЗИ должна быть санкционирована соответствующим органом криптографической защиты.

Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих сведений об уникальной последовательности символов, предназначенных для создания СКЗИ (криптоключей).

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать в соответствующий орган криптографической защиты.

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях специального назначения пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае пользователи СКЗИ по согласованию с органом криптографической защиты обязаны предусмотреть организационно - технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

Режим охраны помещений специального назначения пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации по согласованию с соответствующим органом криптографической защиты. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения Инструкции № 152, специфику и условия работы конкретных пользователей СКЗИ.

В помещениях специального назначения пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения специального назначения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации руководителю органа криптографической защиты. Прибывшие сотрудники органа криптографической защиты должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

ФОРМА ЖУРНАЛА
ПОЭКЗЕМПЛЯРНОГО УЧЕТА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ), ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ
В ЛОГАУ «Кингисеппский ЦСО»

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1		3	4	5	6	7	8	9	10	11	12	13	14	15

ФОРМА ЖУРНАЛА УЧЕТА ВЫДАЧИ МАШИННЫХ НОСИТЕЛЕЙ
В ЛОГАУ «Кингисеппский ЦСО»

№ п/п	Дата	Наименование материальной ценности (МЦ)	Марка, модель МЦ	Ф.И.О. сотрудника, получившего МЦ	Подпись сотрудника, получившего МЦ
1	2	3	4	5	6

ФОРМА ЖУРНАЛА
УЧЕТА РАБОТНИКОВЛОГАУ «Кингисеппский ЦСО», ДОПУЩЕННЫХ К РАБОТЕ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ)

№ п/п	Ф.И.О. сотрудника, допущенного к СКЗИ	Сведения о допуске		Сведения о проведении обучения		Сведения о прекращении допуска		Примечание
		Дата допуска	Ф.И.О., должность, подпись должностного лица, осуществившего допуск	Дата проведения обучения сотрудника допущенного к СКЗИ	Ф.И.О., должность, подпись должностного лица, проводившего обучение	Дата прекращения допуска	Ф.И.О., должность, подпись должностного лица, прекратившего допуск	
1	2	3	4	5	6	7	8	9

ФОРМА ЖУРНАЛА
ОЗНАКОМЛЕНИЯ РАБОТНИКОВ ЛОГАУ «Кингисеппский ЦСО» С НОРМАТИВНОЙ ДОКУМЕНТАЦИЕЙ В ОБЛАСТИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Ф.И.О. должностного лица работника	Наименование документа (или номера распоряжения, которыми утверждены документы)	Дата ознакомления	Подпись лица, которое было ознакомлено с документами	Ф.И.О. лица, проводившего ознакомление	Примечание
1	2	3	4	5	6	7

ФОРМА ЖУРНАЛА
УЧЕТА МЕРОПРИЯТИЙ ПО КОНТРОЛЮ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ ПО ОБРАБОТКЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА (ПЕРСОНАЛЬНЫХ ДАННЫХ)

№ п/п	Мероприятие	Дата проведения мероприятия	Ф.И.О. и подпись исполнителя, проводившего мероприятие	Результаты проведения мероприятия	Примечание
1	2	3	4	5	6

ФОРМА ЖУРНАЛА
УЧЕТА СЕЙФОВ, МЕТАЛЛИЧЕСКИХ ШКАФОВ, СПЕЦИАЛЬНЫХ ХРАНИЛИЩ И КЛЮЧЕЙ ОТ НИХ

№ п/п	Учетный номер сейфа/металлического шкафа/специального хранилища	Наименование хранилища (сейф, металлический шкаф, специальное хранилище)	Заводской инвентарный номер хранилища	Состав хранимого имущества (документы, носители)	Место нахождения хранилища	Ф.И.О. лица, ответственного за хранилище	Кол-во компонентов ключей и их номера	Дата и расписка ответственного за хранилище в получении ключей	Дата и расписка сотрудника получившего комплект ключей, с указанием номера комплекта
1	2	3	4	5	6	7	8	9	10