

Политика обработки персональных данных в ФГБУ «СКК «Анапский» МО РФ

I. Общие положения

1. Политика обработки персональных данных в ФГБУ «СКК «Анапский» МО РФ (далее - Политика) устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются в ФГБУ «СКК «Анапский» МО РФ, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. Настоящие Политика определяют политику ФГБУ «СКК «Анапский» МО РФ как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

3. Обработка персональных данных в ФГБУ «СКК «Анапский» МО РФ (далее - оператор) осуществляется с соблюдением принципов и условий, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2018, № 1, ст. 82) (далее - Федеральный закон "О персональных данных") и настоящими Политикой.

II. Категории субъектов персональных данных

4. Оператором обрабатываются персональные данные следующих категорий субъектов персональных данных:

- 1) работников ФГБУ «СКК «Анапский» МО РФ;
- 2) граждан, претендующих на замещение должностей работников ФГБУ «СКК «Анапский» МО РФ (далее - кандидаты);
- 3) лиц, состоящих в родстве (свойстве) с субъектами персональных данных, указанными в подпунктах 1, 2 данного пункта, в случаях, предусмотренных законодательством Российской Федерации;
- 4) уволенных из ФГБУ «СКК «Анапский» МО РФ в течение ____ лет со дня исключения их из списков сотрудников;
- 5) физических лиц и представителей организаций, обратившихся в ФГБУ «СКК «Анапский» МО РФ за предоставлением (исполнением) государственных услуг;
- 6) граждан, обратившихся в ФГБУ «СКК «Анапский» МО РФ в соответствии с Федеральным законом от 2 мая 2006 г. № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" (Собрание законодательства Российской Федерации, 2006, № 19, ст. 2060; 2018, № 53, ст. 8454);
- 7) посетители объектов ФГБУ «СКК «Анапский» МО РФ;
- 8) пользователи официальных сайтов ФГБУ «СКК «Анапский» МО РФ в

информационно-телекоммуникационной сети "Интернет";

9) работников, посетителей сайта, заказчиков, а также персональные данные других субъектов персональных данных, полученные от контрагентов, необходимые для оказания услуги, исполнения соглашения или договора, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

III. Цели обработки персональных данных

5. Обработка персональных данных организуется оператором в целях:

1) предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ФГБУ «СКК «Анапский» МО РФ функций, полномочий и обязанностей;

2) обеспечения служебных и трудовых отношений, а также кадровой работы;

3) обеспечения заработной платой работников ФГБУ «СКК «Анапский» МО РФ, медицинским обеспечением личного состава ФГБУ «СКК «Анапский» МО, а также предоставления им иных социальных гарантий;

4) предоставления (исполнения) ФГБУ «СКК «Анапский» МО РФ услуг (функций);

5) противодействия коррупции;

6) оформления допуска к служебной (государственной) тайне;

7) осуществления медицинских осмотров в связи с поступлением на работу в ФГБУ «СКК «Анапский» МО РФ, ее прохождением и увольнением с нее;

8) обеспечения своевременного и в полном объеме рассмотрения обращений граждан Российской Федерации в порядке, установленном Федеральным законом от 2 мая 2006 г. № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации";

9) соблюдения пропускного режима на объектах ФГБУ «СКК «Анапский» МО РФ;

10) обработки обращений пользователей официальных сайтов ФГБУ «СКК «Анапский» МО РФ в информационно-телекоммуникационной сети "Интернет", направленных в форме электронного документа.

6. В ФГБУ «СКК «Анапский» МО РФ обрабатываются следующие персональные данные:

1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилия, имя, отчество (при наличии), дата, причина их изменения);

2) дата (число, месяц и год рождения) и место рождения;

3) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи;

4) сведения о гражданстве (какого государства, если изменялось, то когда и по какой причине);

5) адрес и дата регистрации по месту жительства (месту пребывания),

адрес фактического проживания (пребывания);

6) номера телефонов (домашнего, служебного, сети подвижной радиотелефонной связи);

7) адрес электронной почты;

8) идентификационный номер налогоплательщика;

9) реквизиты страхового свидетельства обязательного пенсионного страхования;

10) реквизиты страхового медицинского полиса обязательного медицинского страхования;

11) личный номер военнослужащего;

12) сведения, содержащиеся в водительском удостоверении (серия, номер, кем и когда выдано);

13) сведения об образовании (наименование образовательной организации и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки, специальность и квалификация по документу об образовании);

14) сведения о наличии ученой степени, ученого звания (дата присвоения, реквизиты диплома, аттестата);

15) реквизиты паспорта гражданина Российской Федерации, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации (при наличии);

16) сведения о владении иностранными языками (какими);

17) сведения о присвоении спортивного звания, спортивного разряда;

18) фотографии (для формирования личного дела, оформления служебного удостоверения, формирования анкет, установленных законодательством Российской Федерации);

19) сведения о национальной принадлежности;

20) отношение к исполнению воинской обязанности, сведения, содержащиеся в документах воинского учета (для граждан, пребывающих в запасе Вооруженных Сил, и лиц, подлежащих призыву на военную службу);

21) информация о прохождении военных сборов;

22) реквизиты документа, подтверждающего право на меры социальной поддержки;

23) сведения об участии в боевых действиях, нахождении в плену, полученных ранениях;

24) сведения о наличии званий "Ветеран труда", "Ветеран военной службы", "Ветеран боевых действий" и реквизиты удостоверений, подтверждающих наличие указанных званий;

25) занимаемая должность, с какого времени;

26) классный чин федеральной государственной гражданской службы, воинское звание (кем и когда присвоены);

27) сведения о присвоении квалификационного звания, классной квалификации (основание и дата присвоения);

28) сведения о трудовой деятельности (включая работу по совместительству, предпринимательскую деятельность и иную деятельность), сведения о прохождении военной (федеральной государственной гражданской)

службы;

29) сведения о врученных государственных наградах, иных наградах и знаках отличия (основание и дата награждения);

30) сведения о военно-учетных специальностях;

31) сведения о семейном положении (состав семьи);

32) реквизиты свидетельств государственной регистрации актов гражданского состояния (номер и дата составления акта) и содержащиеся в них сведения;

33) реквизиты свидетельства о рождении (усыновлении) детей (серия, номер, кем и когда выдано);

34) сведения о наличии (отсутствии) жилых помещений, принадлежащих субъекту персональных данных на праве собственности;

35) сведения о присвоенном регистрационном номере в реестре участников накопительно-ипотечной системы жилищного обеспечения военнослужащих;

36) сведения, содержащиеся в выписке из домовой книги, копиях финансового лицевого счета;

37) сведения о своих доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера своих супругов (супругов) и несовершеннолетних детей в соответствии с Федеральным законом от 25 декабря 2008 г. № 273-ФЗ "О противодействии коррупции" (Собрание законодательства Российской Федерации, 2008, № 52, ст. 6228; 2019, № 30, ст. 4153);

38) сведения о счетах в банках и иных кредитных организациях (наименование банка или кредитной организации, номер счета и дата открытия), реквизиты банковских карт (номер карты);

39) сведения о результатах медицинского освидетельствования (военно-врачебной экспертизы);

40) сведения о допуске к служебной (государственной) тайне, оформленном за период работы, службы, учебы (форма, номер и дата);

41) сведения о пребывании за границей (когда, где, с какой целью);

42) фамилии, имена, отчества (при наличии), отца, матери, братьев, сестер, детей, супруга (супруги), в том числе бывших, субъекта персональных данных, а также супруги братьев и сестер, братьев и сестер супруга (супруги) (при изменении фамилии, имени, отчества (при наличии) - прежние фамилия, имя, отчество (при наличии), даты рождения;

43) место рождения, место работы, адрес регистрации по месту жительства (месту пребывания), адрес фактического места жительства отца, матери, братьев, сестер, детей, супруга (супруги), в том числе бывших, субъекта персональных данных, а также супруги братьев и сестер, братьев и сестер супруга (супруги);

44) сведения о постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство отце, матери, братьях, сестрах, детях, супруге, в том числе бывших супругах (фамилия, имя, отчество (при наличии), а также супруги братьев и сестер, братьев и сестер супруга (супруги), с какого времени проживают за

границей);

45) информация о наличии либо отсутствии судимости (в том числе снятой или погашенной) (исключительно в случаях и в порядке, которые определяются в соответствии с федеральными законами);

46) иные сведения, которые субъект персональных данных пожелал сообщить о себе и которые отвечают целям их обработки.

Обработка Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается в случаях, предусмотренных пунктом 4 статьи 10 ФЗ-152.

7. В ФГБУ «СКК «Анапский» МО РФ для каждой цели обработки персональных данных, указанной в пункте 5 Правил, начальником подразделения, обрабатывающим персональные данные по согласованию с руководителем устанавливается объем обрабатываемых персональных данных.

IV. Обработка и защита персональных данных от несанкционированного доступа, неправомерного использования и утраты

8. Обработка персональных данных оператором осуществляется при наличии письменного согласия субъекта персональных данных на обработку его персональных данных в соответствии со статьей 9 Федерального закона "О персональных данных", а также без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона "О персональных данных", при этом:

1) обработка персональных данных в целях, указанных в подпункте 1 пункта 5 Правил, осуществляется без согласия субъекта персональных данных в соответствии с пунктом 2 части 1 статьи 6, пунктами 2.1, 7 части 2 статьи 10 и частью 2 статьи 11 Федерального закона "О персональных данных";

2) обработка персональных данных в целях, указанных в подпункте 2 пункта 5 Правил, осуществляется при наличии полученного согласия субъекта персональных данных на обработку его персональных данных в письменной форме в соответствии с пунктом 1 части 1 статьи 6, пунктом 1 части 2 статьи 10 и частью 1 статьи 11 Федерального закона "О персональных данных";

3) обработка персональных данных в целях, указанных в подпункте 3 пункта 5 Правил, осуществляется при наличии полученного согласия субъекта персональных данных на обработку его персональных данных в письменной форме в соответствии с пунктом 1 части 1 статьи 6 и без согласия субъекта персональных данных в соответствии с пунктом 6 части 1 статьи 6, пунктами 2.3, 3 и 4 части 2 статьи 10 Федерального закона "О персональных данных";

4) обработка персональных данных в целях, указанных в подпункте 4 пункта 5 Правил, осуществляется без согласия субъекта персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона "О персональных данных";

5) обработка персональных данных в целях, указанных в подпункте 5 пункта 5 Правил, осуществляется без согласия субъекта персональных данных

в соответствии с пунктами 2 и 11 части 1 статьи 6 Федерального закона "О персональных данных";

6) обработка персональных данных в целях, указанных в подпункте 6 пункта 5 Правил, осуществляется при наличии полученного согласия субъекта персональных данных на обработку его персональных данных в письменной форме в соответствии с пунктом 1 части 1 статьи 6 Федерального закона "О персональных данных";

7) обработка персональных данных в целях, указанных в подпункте 7 пункта 5 Правил, осуществляется при наличии полученного согласия субъекта персональных данных на обработку его персональных данных в письменной форме в соответствии с пунктом 1 части 1 статьи 6 и без согласия субъекта персональных данных в соответствии с пунктом 4 части 2 статьи 10 Федерального закона "О персональных данных";

8) обработка персональных данных в целях, указанных в подпункте 8 пункта 5 Правил, осуществляется без согласия субъекта персональных данных в соответствии с пунктом 2 части 1 статьи 6 Федерального закона "О персональных данных";

9) обработка персональных данных в целях, указанных в подпункте 9 пункта 5 Правил, осуществляется без согласия посетителей объектов Вооруженных Сил в соответствии с пунктом 7 части 1 статьи 6 Федерального закона "О персональных данных";

10) обработка персональных данных в целях, указанных в подпункте 10 пункта 5 Правил, осуществляется при наличии полученного в электронной форме согласия субъекта персональных данных на обработку его персональных данных в соответствии с пунктом 1 части 1 статьи 6 Федерального закона "О персональных данных".

9. Получение согласия в письменной форме субъекта персональных данных на обработку персональных данных осуществляется должностными лицами, указанными в перечне должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в ФГБУ «СКК «Анапский» МО РФ (далее - должностные лица), утверждаемом в соответствии с подпунктом "б" пункта 1 перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, посредством предоставления субъектам персональных данных для ознакомления и подписания Типовой формы согласия на обработку персональных данных субъектов персональных данных в Вооруженных Силах Российской Федерации (далее - Типовая форма согласия).

10. Данное субъектом персональных данных согласие на обработку персональных данных действует:

1) для работников ФГБУ «СКК «Анапский» МО РФ - со дня предоставления ими согласия на обработку персональных данных на время прохождения работы;

2) для иных субъектов персональных данных - со дня предоставления ими согласия на обработку персональных данных до достижения целей обработки персональных данных.

Действие данного субъектом персональных данных согласия на обработку персональных данных также прекращается в случае его отзыва субъектом персональных данных в соответствии с пунктом 12 Правил.

11. Согласие на обработку персональных данных подписывается субъектом персональных данных в день рассмотрения и подписания им контракта о прохождении военной службы (служебного контракта, контракта, трудового договора) или в день предоставления уполномоченными должностными лицами Типовой формы согласия для рассмотрения и подписания субъектом персональных данных (его законным представителем).

12. Подписанное субъектом персональных данных согласие на обработку персональных данных может быть отозвано субъектом персональных данных только посредством направления им письменного заявления (заявления в форме электронного документа, подписанного в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2016, № 26, ст. 3889) в ФГБУ «СКК «Анапский» МО РФ.

13. При отказе субъекта персональных данных подписать согласие на обработку персональных данных должностные лица продолжают обработку персональных данных без согласия субъекта персональных данных по основаниям, указанным в пункте 8 Правил.

14. Одновременно с предоставлением Типовой формы согласия субъекту персональных данных доводится под подпись Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные Вооруженным Силам Российской Федерации (далее - Типовая форма разъяснения).

15. Кандидатам, подписавшим Типовую форму согласия и (или) Типовую форму разъяснения и впоследствии заместившим должности работников ФГБУ «СКК «Анапский» МО РФ, формы для повторного рассмотрения и подтверждения (подписания) не представляются и названными лицами не подписываются, а включаются в их личные дела.

16. При назначении работника на должность, замещение которой предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, такому субъекту персональных данных отделом кадров (назначенным должностным лицом), доводится под подпись типовое обязательство должностного лица, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним контракта (служебного контракта или трудового договора) прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных (служебных) обязанностей в Вооруженных Силах Российской Федерации.

17. Оригиналы подписанных субъектами персональных данных (их законными представителями) Типовых форм согласия, Типовых форм разъяснения и Типовых обязательств хранятся в их личных делах, в том числе в личных делах кандидатов, которым было отказано в приеме на работу, и субъектам персональных данных (их законным представителям) не выдаются (не возвращаются), а также из указанных дел не изымаются.

18. В случае подачи оператору субъектом персональных данных письменного заявления об отзыве субъектом персональных данных согласия на обработку его персональных данных уполномоченные должностные лица направляют субъекту персональных данных письменное извещение (письмо), в котором указывают, что оператор признает отозванной подписанное субъектом персональных данных согласие на обработку персональных данных, но при этом сохраняет за собой право на обработку персональных данных субъекта персональных данных в соответствии с пунктом 8 Правил.

19. Если предоставление персональных данных субъектом персональных данных является обязательным требованием в соответствии с законодательством Российской Федерации, должностное лицо разъясняет субъекту персональных данных юридические последствия его отказа предоставить свои персональные данные.

20. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", должностные лица обязаны обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2 - 4, 8 части 1 статьи 6 Федерального закона "О персональных данных".

21. При осуществлении оператором записи персональных данных в информационных системах обеспечивается конфиденциальность персональных данных при их обработке как в указанных информационных системах, так и вне таких систем.

22. Систематизация персональных данных осуществляется путем обработки и анализа накопленных сведений о субъектах персональных данных.

23. Целью систематизации является обеспечение возможности в соответствии с заданным алгоритмом осуществлять поиск и доступ к персональным данным, зафиксированным на бумажных, электронных и магнитных носителях информации, а также содержащимся в картотеках (бумажных, электронных, магнитных) и базах данных, используемых в информационных системах персональных данных.

24. Персональные данные, систематизированные в информационных системах персональных данных, подлежат накоплению для достижения полноты и достоверности обрабатываемых персональных данных.

25. Накопление персональных данных осуществляется путем сбора их должностными лицами из различных источников информации, а также последующего внесения в них информации, касающейся субъектов персональных данных в связи с осуществлением трудовой деятельности.

26. Уточнение (обновление, изменение) персональных данных осуществляется путем выявления (подтверждения) наличия неточных персональных данных и последующего выполнения действий (операций) по их обновлению и изменению.

27. Должностные лица, получившие доступ к персональным данным, для обеспечения законной передачи персональных данных в случаях, соответствующих целям обработки:

1) осуществляют передачу персональных данных в пределах ФГБУ «СКК «Анапский» МО РФ;

2) не предоставляют персональные данные третьим лицам без согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;

3) предупреждают лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они переданы, а также требуют от этих лиц подтверждения того, что это правило соблюдено;

4) распространяют персональные данные в общедоступных источниках, в том числе в информационно-телекоммуникационной сети "Интернет" и иных средствах массовой информации при доказательстве получения согласия субъекта персональных данных в письменной форме на указанное распространение персональных данных с учетом выполнения требований, предъявляемых к таким персональным данным (в части их предназначения, содержания и непринадлежности к персональным данным, подлежащим обезличиванию), за исключением случаев обязательного распространения (опубликования) персональных данных в средствах массовой информации в соответствии с законодательством Российской Федерации;

5) при передаче персональных данных в информационных системах персональных данных применяют технологии, обеспечивающие их защиту от несанкционированного (неправомерного или случайного) доступа, от уничтожения, изменения, блокирования, копирования, предоставления и распространения, в том числе с использованием шифровальных (криптографических) средств, при этом обработку персональных данных в информационных системах персональных данных производят только в информационно-телекоммуникационных сетях, физически изолированных от информационно-телекоммуникационных сетей общего пользования, а их передачу по незащищенным каналам связи допускают только при использовании шифровальных (криптографических) средств.

28. Субъект персональных данных имеет право на доступ к своим персональным данным, в том числе на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации (Часть 1 статьи 14 Федерального закона "О персональных данных").

29. Обработка персональных данных без использования средств автоматизации осуществляется с учетом требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" (Собрание законодательства Российской Федерации, 2008, № 38, ст. 4320).

30. Обеспечение внешней защиты персональных данных достигается:

1) установлением пропускного режима и особого порядка приема, учета и контроля посетителей;

2) использованием технических средств охраны;

3) применением программно-технических комплексов защиты

информации, содержащейся на электронных и магнитных носителях информации.

31. Обеспечение внутренней защиты персональных данных достигается:

- 1) ограничением и регламентацией состава должностных лиц, должностные обязанности которых требуют доступа к персональным данным;
- 2) избирательным и обоснованным распределением (разделением) доступа должностных лиц к персональным данным и материальным носителям информации, которые их содержат;
- 3) рациональным размещением рабочих мест, на которых обрабатываются персональные данные, в целях исключения бесконтрольной обработки персональных данных;
- 4) регулярными проверками должностных лиц на знание ими требований нормативных правовых актов Российской Федерации в области обработки персональных данных и обеспечения безопасности информации (защиты персональных данных);
- 5) формированием условий, необходимых для работы с материальными носителями информации, базами персональных данных, в том числе персональными данными, содержащимися на машинных носителях информации, используемых в информационных системах персональных данных;
- 6) утверждением списков (перечней) должностных лиц (субъектов персональных данных), имеющих право доступа в помещения, в которых обрабатываются и (или) хранятся персональные данные;
- 7) выявлением нарушений при осуществлении обработки персональных данных, в том числе связанных с нарушением требований к защите персональных данных и обеспечению безопасности информации, а также их устранением;
- 8) проведением профилактической работы с должностными лицами, имеющими доступ к персональным данным, направленной на предупреждение случаев несанкционированной передачи таких данных.

32. При осуществлении обработки персональных данных без использования средств автоматизации должностные лица выполняют следующие действия:

- 1) обеспечивают раздельное хранение персональных данных, обработка которых предусмотрена в различных целях, в том числе не допускают их фиксации на одном материальном носителе информации, если цели сбора или обработки персональных данных заведомо несовместимы, и обособляют персональные данные, в частности путем их записи в специальных разделах или на полях;
- 2) создают условия, обеспечивающие сохранность персональных данных и исключение случаев несанкционированного (неправомерного или случайного) доступа к ним;
- 3) производят уточнение персональных данных, подлежащих обработке, путем их обновления (изменения);
- 4) осуществляют контроль в части, их касающейся, за соблюдением порядка отбора персональных данных к уничтожению, уничтожения и (или) обезличивания персональных данных.

33. Организация защиты персональных данных при обработке в информационных системах персональных данных (с использованием средств автоматизации) осуществляется с учетом положений пунктов 34 - 43 настоящих Правил.

34. Безопасность персональных данных при их обработке в информационных системах персональных данных должна обеспечиваться с помощью системы защиты персональных данных, нейтрализующей угрозы безопасности персональных данных, актуальные при их обработке, путем исключения несанкционированного доступа к персональным данным (далее - система защиты персональных данных).

35. Система защиты персональных данных оператором включает организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также современные информационные технологии, применяемые в информационных системах персональных данных.

36. При обработке персональных данных в информационных системах персональных данных применяются меры по обеспечению их безопасности, установленные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (зарегистрирован Министерством юстиции Российской Федерации 14 мая 2013 г., регистрационный № 28375) (с изменениями, внесенными приказом Федеральной службы по техническому и экспортному контролю от 23 марта 2017 г. № 49 (зарегистрирован Министерством юстиции Российской Федерации 25 апреля 2017 г., регистрационный № 46487).

37. Определение типа угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных, производится в соответствии с пунктом 5 части 1 статьи 18.1 и части 5 статьи 19 Федерального закона "О персональных данных" с учетом оценки возможного вреда, к которому могут привести указанные угрозы.

38. Требуемый уровень защищенности персональных данных при их обработке в информационных системах персональных данных обеспечивается в соответствии с требованиями к защите информации, определяемыми в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2019, № 18, ст. 2214), а также требованиями к защите персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

39. Для обеспечения требуемого уровня защищенности персональных данных, в том числе биометрических персональных данных, соответствующего требованиям к защите персональных данных, применяются следующие организационные, технические и иные меры по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных:

1) определение по каждой информационной системе персональных данных, эксплуатируемой в ФГБУ «СКК «Анапский» МО РФ решением начальника, должностного лица, ответственного за эксплуатацию (обеспечение функционирования) и выполнение мер по обеспечению безопасности персональных данных при их обработке;

2) организация режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего неконтролируемому проникновению или пребыванию в этих помещениях посторонних лиц, не имеющих права доступа в эти помещения;

3) осуществление учета машинных носителей информации, а также выполнение мер, направленных на обеспечение их сохранности;

4) организация режима доступа к обрабатываемым персональным данным в информационных системах персональных данных;

5) осуществление мониторинга обработки персональных данных для обнаружения фактов несанкционированного доступа к ним, выявление модифицированных или уничтоженных персональных данных вследствие несанкционированного доступа к ним для их последующего восстановления;

6) применение в информационных системах персональных данных только технических и программных средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

7) осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

8) осуществление внутреннего контроля принимаемых мер по обеспечению безопасности персональных данных, в том числе выполнения требуемого уровня защищенности информационных систем персональных данных и персональных данных, обрабатываемых без использования средств автоматизации.

40. В целях обеспечения надлежащей эксплуатации информационных систем персональных данных в ФГБУ «СКК «Анапский» МО РФ осуществляется:

1) определение уровней защищенности персональных данных в информационных системах в соответствии с Требованиями к защите персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

2) проведение комплекса организационных и технических мер по обеспечению безопасности персональных данных с учетом уровня защищенности персональных данных в информационных системах и актуальных угроз безопасности персональных данных (при их обработке в информационных системах персональных данных) в виде системы защиты персональных данных в соответствии с требованиями законодательства Российской Федерации в области обеспечения безопасности информации, в том

числе в связи с использованием в ФГБУ «СКК «Анапский» МО РФ информационно-телекоммуникационной сети "Интернет" (Указ Президента Российской Федерации от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (Собрание законодательства Российской Федерации, 2008, № 12, ст. 1110; 2015, № 21, ст. 3092), Указ Президента Российской Федерации от 22 мая 2015 г. № 260 "О некоторых вопросах информационной безопасности Российской Федерации" (Собрание законодательства Российской Федерации, 2015, № 21, ст. 3092).

41. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми в соответствии с частью 4 статьи 19 Федерального закона "О персональных данных".

42. Вывод на печать документов, содержащих персональные данные, с помощью средств автоматизации, входящих или не входящих в состав информационных систем персональных данных, допускается в целях обработки в связи с исполнением служебных (трудовых) обязанностей, в том числе для передачи их печатных копий субъектам персональных данных, персональные данные которых они содержат, либо должностным лицам, допущенным к обработке персональных данных.

43. Оператор обязан не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом Статья 7 Федерального закона "О персональных данных".

V. Хранение персональных данных, сроки их обработки и хранения

44. Хранение персональных данных осуществляется на бумажном носителе в подразделениях ФГБУ «СКК «Анапский» МО РФ в функции которых входит обработка персональных данных, и в электронном виде в автоматизированных электронных системах.

45. Сроки обработки и хранения персональных данных в Вооруженных Силах определяются в соответствии с законодательством Российской Федерации.

Срок хранения персональных данных, внесенных в автоматизированные информационные системы, должен соответствовать сроку хранения персональных данных на бумажных носителях.

46. Если сроки обработки и хранения персональных данных не установлены федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, то обработка и хранение персональных данных субъектов, персональные данные которых обрабатываются в ФГБУ «СКК «Анапский» МО РФ, осуществляются не дольше, чем этого требуют цели их обработки и хранения (Пункт 7 статьи 5 Федерального закона "О персональных данных").

47. Персональные данные при их обработке, осуществляемой без использования автоматизированных информационных систем, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях.

Хранение персональных данных, обработка которых осуществляется в различных целях, определенных настоящими Политиками, осуществляется отдельно на разных материальных носителях персональных данных.

VI. Уничтожение персональных данных при достижении целей обработки или при наступлении иных законных оснований

48. Уничтожению подлежат обрабатываемые персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом "О персональных данных".

Уничтожение персональных данных осуществляется в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных (Пункт 4 статьи 21 Федерального закона "О персональных данных").

49. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных прекращается их обработка и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, они уничтожаются в срок, не превышающий 30 дней с даты поступления указанного отзыва.

50. В случае отсутствия возможности уничтожения персональных данных в течение 30 дней осуществляется блокирование таких персональных данных с последующим их уничтожением в срок не более чем шесть месяцев.

51. Уничтожение документов, содержащих персональные данные, производится путем сжигания, стирания с материальных носителей или с помощью бумагорезательной машины.

Уничтожение электронных носителей, содержащих персональные данные, производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

Результаты уничтожения носителей персональных данных оформляются актом об их уничтожении, который хранится в течение одного года после уничтожения в структурном подразделении (должностным лицом) воинской части, осуществляющем обработку персональных данных.

52. Архивные документы, содержащие персональные данные на бумажном носителе, по истечении срока хранения в ФГБУ «СКК «Анапский» МО РФ передаются на хранение в Центральный архив Министерства обороны Российской Федерации.

VII. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

53. Для выявления и предотвращения нарушений, предусмотренных законодательством Российской Федерации в сфере персональных данных, в ФГБУ «СКК «Анапский» МО РФ проводятся следующие процедуры:

1) осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

2) организация и проведение периодических проверок условий обработки персональных данных, определение по результатам указанных проверок мер, необходимых для устранения выявленных нарушений в соответствии с подпунктом "д" пункта 1 постановления № 211;

3) оценка вреда, который может быть причинен субъектам персональных данных;

4) прекращение обработки персональных данных при достижении конкретных целей, определенных настоящими Политиками;

5) недопущение обработки персональных данных, не совместимой с целями сбора персональных данных, объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой;

6) соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки. Устранение избыточности состава, содержания, объема обрабатываемых персональных данных заявленным целям;

7) обеспечение при обработке персональных данных точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных.