Подписано цифровой подписью: Царёв Иван Николаевич
DN: c=RU, st=г. Санкт-Петербург, l=Петергоф, title=Начальник, o=ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "САНКТ-ПЕТЕРБУРГСКИЙ КАДЕТСКИЙ ВОЕННЫЙ КОРПУС ИМЕНИ КНЯЗЯ АЛЕКСАНДРА НЕВСКОГО МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ", 1.2.643.100.3=120B313536333683334343931, 1.2.643.3.131.1.1=120C313130333035333638393434, email=finkad@mail.ru, givenName=Иван Николаевич, sn=Царёв, cn=Царёв Иван Николаевич
Местонахождение: г.Петергоф

Приложение № 1
к приказу начальника СПбКВК
31.08.2023 года №145

ПОЛОЖЕНИЕ
О защите персональных данных сотрудников и воспитанников СПбКВК

I. Общие положения

1. Целью данного Положения является защита персональных данных сотрудников и воспитанников от несанкционированного доступа, неправомерного их использования или утраты.

2. Настоящее Положение разработано на основании статей Конституции Российской Федерации, Трудового Кодекса Российской Федерации, Кодекса об административных правонарушениях Российской Федерации, Гражданского Кодекса Российской Федерации, Уголовного Кодекса Российской Федерации, Руководства по защите информации от несанкционированного доступа в Вооруженных Силах Российской Федерации, утвержденного приказом Министра обороны Российской Федерации от «09» февраля 2013г. № 011, Инструкции по организации в Вооруженных Силах Российской Федерации защиты информации ограниченного доступа, не содержащих сведений, составляющих государственную тайну, обрабатываемой в государственных системах и информационных системах персональных данных, утвержденной приказом Министра обороны Российской Федерации от 2014г. № 925дсп, Инструкции по организации защиты информации при подключении и использовании информационно-телекоммуникационных сетей общего пользования в Вооруженных Силах Российской Федерации, утвержденной приказом Министра обороны Российской Федерации от 2012г. № 950, а также Федерального закона «Об информации, информатизации и защите информации».

3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

4. Настоящее Положение утверждается и вводится в действие приказом начальника СПбКВК и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным сотрудников.

II. Понятие и состав персональных данных

5. Персональные данные работника или воспитанника информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного сотрудника или воспитанника. Под информацией понимаются сведения о фактах, событиях и обстоятельствах жизни сотрудника или воспитанника, позволяющие идентифицировать его личность.

6. В состав персональных данных сотрудника или воспитанника входят:

анкетные и биографические данные;

образование;
сведения о трудовом и общем стаже;
сведения о составе семьи;
паспортные данные;
сведения о воинском учете;
сведения о заработной плате сотрудника;
сведения о социальных льготах;
специальность,
занимаемая должность;
наличие судимостей;
адрес места жительства;
домашний телефон;
содержание трудового договора;
подлинники и копии приказов по личному составу;
личные дела и трудовые книжки сотрудников;
основания к приказам по личному составу;
дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
копии отчетов, направляемые в органы статистики.

7. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения соответствующий гриф ограничения на них не ставится.

III. Обработка персональных данных

8. Под обработкой персональных данных сотрудника или воспитанника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных.

9. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных сотрудника или воспитанника обязаны соблюдать следующие общие требования:

обработка персональных данных сотрудника или воспитанника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудника или воспитанника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

при определении объема и содержания обрабатываемых персональных данных сотрудника или воспитанника администрация СПбКВК должна руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

получение персональных данных может осуществляться как путем представления их самим сотрудником или законным представителем воспитанника, так и путем получения их из иных источников.

персональные данные следует получать у него самого. Если персональные данные сотрудника или воспитанника возможно получить только у третьей стороны, то сотрудник или законный представитель воспитанника должен быть

уведомлен об этом заранее и от него должно быть получено письменное согласие. Администрация СПбКВК должна сообщить сотруднику или законному представителю воспитанника о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа сотрудника или законного представителя воспитанника дать письменное согласие на их получение.

администрация СПбКВК не имеет права получать и обрабатывать персональные данные сотрудника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни сотрудника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны только с его письменного согласия.

администрация СПбКВК не имеет право получать и обрабатывать персональные данные сотрудника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

10. К обработке, передаче и хранению персональных данных сотрудника или воспитанника могут иметь доступ сотрудники СПбКВК.

11. Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

12. Передача персональных данных сотрудника или воспитанника возможна только с их согласия или в случаях, прямо предусмотренных законодательством.

При передаче персональных данных сотрудника или воспитанника администрация СПбКВК должна соблюдать следующие требования:

не сообщать персональные данные сотрудника или воспитанника третьей стороне без письменного согласия сотрудника или законного представителя воспитанника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных Федеральным законом;

не сообщать персональные данные сотрудника или воспитанника в коммерческих целях без его письменного согласия;

предупредить лиц, получающих персональные данные сотрудника или воспитанника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные сотрудника или воспитанника, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Федеральными законами;

разрешать доступ к персональным данным сотрудника или воспитанника только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные сотрудника или воспитанника, которые необходимы для выполнения конкретных функций;

не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции;

передавать персональные данные сотрудника или воспитанника их представителям в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными сотрудника или воспитанника, которые необходимы для выполнения указанными представителями их функций.

Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

При передаче персональных данных сотрудника или воспитанника потребителям (в том числе и в коммерческих целях) за пределы организации, администрация СПбКВК не должна сообщать эти данные третьей стороне без письменного согласия сотрудника или законного представителя воспитанника, за исключением случаев, когда это необходимо в целях предупреждения угрозы их жизни и здоровью или в случаях, установленных федеральным законом.

13. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника или воспитанника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

14. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

15. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

16. При принятии решений, затрагивающих интересы сотрудника, администрация СПбКВК не имеет права основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества сотрудника, его добросовестный и эффективный труд.

IV. Доступ к персональным данным

17. Внутренний доступ (доступ внутри организации). Право доступа к персональным данным сотрудника имеют:

начальник кадетского корпуса;

руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);

при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;

сам сотрудник, носитель данных.

другие сотрудники кадетского корпуса, при выполнении ими своих служебных обязанностей.

Перечень лиц, имеющих доступ к персональным данным сотрудников или воспитанников, определяется ежегодным приказом начальника СПбКВК.

18. Внешний доступ.

К числу массовых потребителей персональных данных вне кадетского корпуса можно отнести государственные и негосударственные функциональные структуры:

налоговые инспекции;

правоохранительные органы;

органы статистики;

страховые агентства;

военкоматы;

органы социального страхования;

пенсионные фонды;

подразделения муниципальных органов управления.

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

19. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

V. Защита персональных данных

20. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

21. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

22. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нару-

шение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и учебной деятельности.

23. Защита персональных данных сотрудника или воспитанника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств, в порядке, установленном федеральным законом.

24. «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

Для обеспечения внутренней защиты персональных данных сотрудников или воспитанников необходимо соблюдать ряд мер:

ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;

строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

знание сотрудником требований нормативно методических документов по защите информации и сохранении тайны;

наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

организация порядка уничтожения информации;

своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;

воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только начальнику СПбКВК, сотрудникам отделения кадров и строевого и, в исключительных случаях, по письменному разрешению начальника СПбКВК, руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

Защита персональных данных сотрудника или воспитанника на электронных носителях.

Все папки, содержащие персональные данные сотрудника или воспитанника, должны быть защищены паролем, который сообщается начальнику отделения кадров и строевого.

25. «Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности СПбКВК, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделении кадров и строевое.

Для обеспечения внешней защиты персональных данных сотрудников или воспитанников необходимо соблюдать ряд мер:

порядок приема, учета и контроля деятельности посетителей;

пропускной режим кадетского корпуса;

учет и порядок выдачи удостоверений;

технические средства охраны, сигнализации;

порядок охраны территории, зданий, помещений, транспортных средств;

требования к защите информации при интервьюировании и собеседованиях.

26. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных сотрудников или воспитанников.

27. По возможности персональные данные обезличиваются.

28. Кроме мер защиты персональных данных, установленных законодательством, работодатели, сотрудники и их представители могут вырабатывать совместные меры защиты персональных данных.

VI. Права и обязанности сотрудника и законного представителя воспитанника

29. Закрепление прав сотрудника или законного представителя воспитанника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

30. Сотрудники и законные представители воспитанника должны быть ознакомлены под расписку с документами СПбКВК, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

31. В целях защиты персональных данных, хранящихся у работодателя, сотрудник или законный представитель воспитанника имеет право:

требовать исключения или исправления неверных или неполных персональных данных;

на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

определять своих представителей для защиты своих персональных данных;

на сохранение и защиту своей личной и семейной тайны.

32. Сотрудник или законный представитель воспитанника обязан:

при приеме на работу сотрудник дает согласие на обработку своих персональных данных подписывая трудовой договор или подписывая отдельное согласие на обработку своих персональных данных (приложение № 1 к настоящему положению);

при приеме на обучение законный представитель воспитанника дает согласие на обработку персональных данных воспитанника подписывая образовательный договор;

передавать администрации СПбКВК или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации;

своевременно сообщать администрации СПбКВК об изменении своих персональных данных.

при увольнении сотрудник делает отзыв согласия на обработку своих персональных данных (приложение № 2 к настоящему положению).

33. Сотрудники и законные представители воспитанника ставят администрацию СПб КВК в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке или других документах на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

34. В целях защиты частной жизни, личной и семейной тайны сотрудники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

VII. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

35. Персональная ответственность одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

36. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

37. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

38. Каждый сотрудник СПбКВК, получающий для работы конфиденциальный документ или доступ к персональным данным в электронном виде,

несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

39. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника или воспитанника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральными законами.

За неисполнение или ненадлежащее исполнение сотрудником, по его вине, возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

Должностные лица, в обязанность которых входит ведение персональных данных сотрудника или воспитанника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на сотрудников.

Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

40. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Начальник лаборатории инновационных образовательных технологий

В.Битюников