

## **ПОЛОЖЕНИЕ** **о порядке организации и проведения работ по защите конфиденциальной информации**

### **I. Общие положения**

1. Настоящее Положение устанавливает порядок организации и проведения работ по защите конфиденциальной информации в муниципальное казенное учреждение дополнительного образования «Одоевская детско-юношеская спортивная школа» (далее – Учреждение).

2. Действие настоящего Положения не распространяется на правоотношения, связанные с обращением со сведениями, составляющими государственную тайну.

3. В настоящем Положении под конфиденциальной информацией (информацией конфиденциального характера, сведениями конфиденциального характера) понимается информация ограниченного доступа, свободный доступ к которой ограничен в соответствии с федеральным законодательством, а также служебная информация, доступ к которой ограничен обладателем информации.

4. В настоящем Положении используются основные понятия в значении, определенном Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также следующие понятия:

автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

допуск к конфиденциальной информации – процедура оформления права граждан на доступ к сведениям конфиденциального характера;

защищаемые помещения (ЗП) – помещения (кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, конференций, переговоров и т.п.), связанных с обсуждением и (или) оглашением информации конфиденциального характера;

контролируемая зона (КЗ) – пространство (территория, здание, помещение или их часть), в котором исключено неконтролируемое пребывание лиц, не имеющих допуска, а также транспортных, технических и иных материальных средств;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональному назначению и техническим характеристикам;

носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку

информационных сигналов;

ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

служебная информация ограниченного распространения – информация, касающаяся деятельности Учреждения, ограничение на распространение которой диктуется служебной необходимостью;

средство защиты информации (СЗИ) – техническое, программное, программно-техническое средство, предназначенное (используемое) для защиты информации;

утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

5. Защита конфиденциальной информации осуществляется на основании действующего законодательства Российской Федерации.

6. Доступ к сведениям конфиденциального характера Учреждение, в том числе содержащимся в информационных системах, может быть предоставлен с согласия обладателя информации и (или) в случаях, установленных законодательством.

7. В Учреждении осуществляется разрешение или ограничение доступа к информации, определяется порядок и условия такого доступа.

8. Сведения конфиденциального характера, в том числе служебную информацию, ставшие известными работнику вследствие выполнения должностных обязанностей, запрещается использовать в личных целях и в целях причинения имущественного ущерба, морального вреда.

## **II. Принципы ограничения доступа к сведениям**

9. Основными принципами ограничения доступа являются законность, обоснованность и своевременность.

10. Законность ограничения доступа заключается в выполнении требований законодательства при отнесении сведений к категории конфиденциальной информации. При этом учитываются как нормы, предписывающие налагать ограничения на доступ к этим сведениям, так и запрещающие такие ограничения.

11. Обоснованность ограничения доступа заключается в установлении путем экспертной оценки целесообразности ограничения доступа, вероятных последствий этого акта, исходя из законных интересов Учреждения.

12. Своевременность ограничения доступа заключается в установлении ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

## **III. Порядок отнесения сведений к категории конфиденциальной информации**

13. Решение об отнесении сведений к категории конфиденциальной информации принимает руководитель Учреждения путем утверждения перечня сведений конфиденциального характера (далее – Перечень сведений).

14. Для включения в Перечень сведений осуществляется анализ информации, содержащейся в утверждаемых руководителем документах, документах текущей деятельности (информационных потоках), обрабатываемых как в интересах обладателя информации, так и в интересах других лиц.

15. С целью обеспечения принципа обоснованности рассматривается возможный ущерб, который может быть нанесен государству, Учреждению, иным лицам в результате разглашения или распространения конфиденциальной информации, с затратами, необходимыми на ограничение доступа к ней.

16. Возможный ущерб оценивается исходя из наличия материальных, финансовых, репутационных и иных рисков или морального вреда в результате несанкционированного разглашения или распространения конфиденциальной информации.

17. При определении размера (степени) ущерба прогнозируются возможные потери и риски, возникающие не только в настоящее время, но и те, которые могут возникнуть в будущем.

18. При рассмотрении вопросов отнесения сведений к категории конфиденциальной информации учитываются следующие отрицательные факторы разглашения конфиденциальной информации:

нарушение федеральных законов и иных нормативных правовых актов по ограничению доступа к информации;

разрыв отношений (или их осложнение) с деловыми партнерами, юридическими и физическими лицами по причине разглашения сведений;

срыв или невыполнение договорных обязательств, контрактов;

создание трудностей при взаимодействии;

экономические, судебные и иные санкции со стороны юридических и физических лиц за незаконное разглашение сведений о них;

потеря, блокирование или искажение информации в базах данных;

несанкционированная передача баз данных или их части;

раскрытие действующей системы защиты информации.

19. Информация, полученная в результате взаимодействия Учреждения с контрагентами в процессе хозяйственной деятельности, может быть отнесена к категории конфиденциальной положениями заключаемых договоров, соглашений, в которых также отражаются взаимные обязательства и ответственность сторон за сохранность этой информации.

Такая информация в Перечень сведений не включается.

#### **IV. Обязанности по защите конфиденциальной информации и ответственность**

20. В Учреждении назначается лица, ответственные:

за организацию обработки персональных данных;

за обеспечение безопасности конфиденциальной информации (в том числе персональных данных), администратор безопасности.

21. Указанные в пункте 20 ответственные лица в пределах своей компетенции организуют:

контролируемый допуск работников Учреждения к информации конфиденциального характера;

учет, хранение и уничтожение документов и машинных носителей с конфиденциальной информацией;

обработку конфиденциальной информации с помощью средств вычислительной техники;

выполнение мероприятий по защите конфиденциальной информации;

контроль соблюдения порядка работы с конфиденциальной информацией.

22. Не допускается хранение и обработка конфиденциальной информации на территории иностранных государств, если иное не предусмотрено действующими международными соглашениями Российской Федерации.

23. Доступ к конфиденциальной информации осуществляется в соответствии с разрешительной системой доступа (матрицей доступа), утверждаемой руководителем Учреждения.

24. За разглашение конфиденциальной информации, а также нарушение порядка обращения с ней, работник Учреждения может быть привлечен к дисциплинарной и (или) иной ответственности, предусмотренной действующим законодательством.

25. Не реже одного раза в год в Учреждении осуществляется контроль (аудит) соблюдения порядка работы с конфиденциальной информацией.

## **V. Порядок обмена конфиденциальной информации**

26. Предоставление (передача) конфиденциальной информации может производиться только на основании решения руководителя Учреждения при условии соблюдения требований по защите информации.

27. Информация конфиденциального характера предоставляется органам государственной власти, государственным учреждениям и органам местного самоуправления Тульской области на безвозмездной основе.

28. Предоставление конфиденциальной информации иным лицам, если иное не установлено законодательством, регулируется заключаемыми договорами, устанавливающими права, обязанности и ответственность сторон, перечень предоставляемых конфиденциальных сведений и компенсацию за разглашение и иное распространение указанных сведений.

29. При направлении сторонним организациям (учреждениям, предприятиям) сведений и документов, содержащих конфиденциальную информацию, в сопроводительном письме необходимо уведомлять (информировать) получателя о законном требовании соблюдения конфиденциальности полученной им информации и ответственности за ее разглашение или распространение. При обмене конфиденциальной информацией между органами власти, учреждениями делать указанное уведомление не обязательно.

30. Передача конфиденциальной информации в электронном виде разрешается только по защищенным каналам связи, оборудованным сертифицированными средствами защиты.

31. Не допускается речевая передача конфиденциальной информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам. При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи.

32. Проведение конфиденциальных мероприятий (в том числе совещаний, комиссий, собраний, обсуждений и т.п.) разрешается только в ЗП, исключающих возможность перехвата речевой информации конфиденциального характера.

33. При необходимости ЗП оборудуются сертифицированными средствами защиты информации. ЗП должны быть аттестованы по требованиям безопасности информации и размещаться в пределах контролируемой зоны органа власти.

34. В Учреждении в соответствии с установленными требованиями по защите информации определяется перечень ЗП и лиц, ответственных за их эксплуатацию.

35. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, устройств сотовой, пейджинговой и транкинговой связи.

## **VI. Организация и проведение работ по защите конфиденциальной информации**

36. Проведение работ по защите конфиденциальной информации осуществляется путем:

выполнения комплекса мероприятий (правовых, организационных, технических), направленных на предотвращение утечки информации (в том числе по техническим каналам), несанкционированного доступа к ней, преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения;

проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации и федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

37. Организация мероприятий по защите конфиденциальной информации возлагается на ответственных лиц, указанных в пункте 20 настоящего Положения.

38. Обработка конфиденциальной информации допускается только на АС Учреждения, оснащенных сертифицированными по требованию законодательства программными, техническими и программно-техническими средствами защиты информации.

39. АС обработки такой информации должны быть аттестованы по требованиям безопасности информации, а применяемое в них программное обеспечение должно быть лицензионным.

40. При обработке конфиденциальной информации с использованием АС необходимо неукоснительно выполнять требования утвержденных руководителем Учреждения локальных актов, регламентирующих:

- антивирусную защиту информации;
- использование программного обеспечения;
- применение машинных носителей информации;
- организацию сетевой защиты информации;
- авторизацию пользователей;
- иные аспекты защиты информации.