ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ ТЫВА
МИНИСТЕРСТВО СПОРТА РЕСПУБЛИКИ ТЫВА

ПРИКАЗ

г. Кызыл

«31» января 2020 г. № 02-13

О назначении ответственного лица по защите информации Министерства спорта Республики Тыва

В соответствии с федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Законом Республики Тыва от 17 января 2013 г. № 1768 ВХ-I «О государственных информационных системах Республики Тыва», а также во исполнение пункта 2 протокола заседания Совета по информационной безопасности при Коллегии по вопросам правоохранительной деятельности, обороны и безопасности в Сибирском федеральном округе от 3 декабря 2018 г. № 21 и пункта 2 решения коллегии Федеральной службы по техническому и экспортному контролю от 18 июля 2018 г. № 62, **ПРИКАЗЫВАЮ:**

1. Утвердить прилагаемую политику информационной безопасности Министерства спорта Республики Тыва (далее – политика информационной безопасности) (приложение № 1).
2. Назначить ответственным лицом за защиту информации в Министерстве спорта Республики Тыва заместителя министра спорта Республики Тыва Оюна Субудая Викторовича;
3. Проводить на регулярной основе с государственными гражданскими служащими Министерства спорта Республики Тыва, осуществляющими обработку информации в государственных информационных системах (пользователями), занятия, в ходе которых информировать их о действующих требованиях по защите информации, типовых нарушениях требований по защите информации, наиболее актуальных угрозах безопасности информации, а также ответственности за нарушения требований по защите информации.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Министр С.Р. Монгуш

Утверждено приказом
Министерства спорта
Республики Тыва
от «31» января 2020 г. № 02-13

ПОЛИТИКА
информационной безопасности Министерства спорта Республики Тыва

I. Общие положения

1. Настоящая политика информационной безопасности Министерства спорта Республики Тыва (далее – политика) разработана в соответствии с:

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 5 декабря 2016 г. № 646;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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 Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

приказом Федеральной службы безопасности России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;

приказом Федеральной службы безопасности России от 19 июня 2019 г. №

282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;

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»;

приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

Законом Республики Тыва от 17 января 2013 г. № 1768 ВХ-I «О государственных информационных системах Республики Тыва».

2. Политика предназначена для обеспечения общих основ информационной безопасности и выбора практических мероприятий по обеспечению и управлению информационной безопасностью в Министерстве спорта Республики Тыва (далее – Министерство) и в подведомственных учреждениях Министерства (далее – учреждения).

3. Министерство и учреждения обязаны соблюдать требования настоящей политики и законодательства Российской Федерации в сфере информационной безопасности.

4. Государственные гражданские служащие Министерства и работники учреждений, ответственные за информационную безопасность, разрабатывают организационно-распорядительную документацию, дополняющую настоящую политику.

II. Объекты защиты

5. Объектами защиты являются: информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

III. Цели и задачи обеспечения информационной безопасности

6. Целью политики информационной безопасности является обеспечение непрерывности работы Министерства и учреждений при выполнении своих полномочий и функций.

7. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих основных свойств объектов защиты:

1) конфиденциальность;

2) целостность;

3) доступность.

8. Необходимый уровень конфиденциальности, целостности и доступности обеспечивается соответствующими множеству значимых факторов, воздействующих на безопасность информации, мерами и средствами обеспечения информационной безопасности.

9. Задачами политики являются:

1) организация системы менеджмента информационной безопасности;

2) своевременное выявление, оценка и прогнозирование факторов, воздействующих на безопасность информации, причин и условий, способствующих нарушению нормального функционирования информационных систем Министерства и учреждений;

3) создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

4) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;

5) защита от несанкционированного доступа к объектам защиты;

6) защита от несанкционированной модификации используемых в информационных системах Министерства и учреждений программных средств, а также защита информационных систем от внедрения несанкционированных программ, включая компьютерные вирусы;

7) определение основных принципов информационной безопасности;

8) определение мер и средств обеспечения информационной безопасности.

10. Поставленные цели и решение задач достигаются:

1) строгим учетом всех объектов защиты;

2) категорированием и классификацией информационных систем и ресурсов для обеспечения защиты на надлежащем уровне;

3) регистрированием действий государственных гражданских служащих Министерства и работников учреждений, осуществляющих обслуживание объектов защиты;

4) распределением обязанностей по обеспечению информационной безопасности. Полномочия работников должны быть четко определены и закреплены должностными регламентами (инструкциями);

5) выполнением всеми пользователями информационных систем Министерства и учреждений требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

6) персональной ответственностью за свои действия каждого работника, имеющего доступ к объектам защиты Министерства и учреждений, в рамках своих функциональных обязанностей;

7) повышением квалификации работников, ответственных за защиту информации в Министерстве и учреждениях;

8) полнотой, реальной выполнимостью и непротиворечивостью требований ор-

ганизационно-распорядительных документов Министерства и учреждений по вопросам обеспечения информационной безопасности;

9) систематической оценкой рисков;

10) непрерывным поддержанием необходимого уровня информационной безопасности Министерства и учреждений;

11) применением физических и технических (программно-аппаратных) средств защиты информационных ресурсов Министерства и учреждений;

12) эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению информационной безопасности.

IV. Система менеджмента информационной безопасности

11. Система менеджмента информационной безопасности предназначена для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы защиты информации в Министерстве и учреждениях при выполнении своих функций.

12. Основные принципы системы менеджмента информационной безопасности:

1) понимание необходимости системы информационной безопасности;

2) назначение ответственности за информационную безопасность;

3) создание административных обязанностей государственных гражданских служащих Министерства и работников учреждений, ответственных за обеспечение информационной безопасности;

4) оценка риска, определяющая соответствующие меры и средства контроля и управления информационной безопасностью;

5) обеспечение комплексного подхода к менеджменту информационной безопасности;

6) выявление и предупреждение инцидентов информационной безопасности;

7) непрерывная переоценка и соответствующая модификация системы информационной безопасности.

13. Для непосредственной организации и эффективного функционирования системы менеджмента информационной безопасности, исключающей возможные конфликты интересов, в Министерстве целесообразно создать подразделение или назначить лицо, ответственное за обеспечение информационной безопасности, и возложить на него решение следующих основных задач:

1) реализация политики информационной безопасности, определение требований к системе защиты информации;

2) анализ текущего состояния обеспечения информационной безопасности;

3) организация мероприятий и координация работ по защите информации всех подразделений Министерства и учреждений;

4) контроль и оценка эффективности применяемых мер и средств защиты информации.

14. Основными функциями подразделений (лиц), ответственных за обеспечение информационной безопасности Министерства и учреждений, являются:

1) формирование требований к системам защиты в процессе создания и дальнейшего развития существующих объектов защиты;

2) подготовка решений по обеспечению конфиденциальности, целостности, доступности объектов защиты;

3) участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;

4) обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;

5) разграничение доступа пользователей к объектам защиты;

6) наблюдение за функционированием системы защиты и ее элементов;

7) проверка надежности функционирования системы защиты;

8) разработка мер нейтрализации моделей возможных атак;

9) обучение сотрудников и работников правилам безопасной обработки информации;

10) контроль соответствия действий администраторов и пользователей установленным правилам обращения с информацией;

11) участие по указанию руководства в служебной проверке по фактам нарушения правил обращения с информацией и оборудованием в учреждениях в соответствии с законодательством Российской Федерации;

12) сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

V. Факторы, воздействующие на безопасность информации

15. Выявление и учет факторов, воздействующих на защищаемую информацию, составляют основу для планирования и проведения эффективных мероприятий по информационной безопасности.

16. Выявление факторов, воздействующих на безопасность информации, должно осуществляться с учетом следующих требований:

1) достаточности уровней классификации факторов, позволяющих формировать их полное множество;

2) гибкость классификации, позволяющей расширять множества классифицируемых факторов, а также вносить необходимые изменения без нарушения структуры классификации.

17. Все множество факторов, воздействующих на защищаемую информацию, по природе их возникновения разделяются на два класса:

1) объективные – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

2) субъективные – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные. Непреднамеренные угрозы вызваны ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п. Преднамеренные угрозы связаны с корыстными, идейными или иными устремлениями людей (злоумышленников).

18. По отношению к объектам защиты факторы разделяются на внутренние и внешние.

19. Основными факторами, воздействующими на безопасность информации, для Министерства и учреждений являются:

1) непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем Министерства и учреждений (в том числе работников, отвечающих за обслуживание и администрирование информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности информационных систем Министерства и учреждений;

2) преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом, халатность и т.п.) действия легально допущенных к информационным ресурсам Министерства и учреждений пользователей (в том числе работников, отвечающих за обслуживание и администрирование информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности информационных систем Министерства и учреждений;

3) деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационных систем Министерства и учреждений;

4) ошибки, допущенные при разработке компонентов информационных систем Министерства и учреждений и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);

5) явления техногенного характера, стихийные бедствия.

20. Реализация основных объективных факторов, воздействующих на безопасность информации, возможна путем:

1) выхода из строя оборудования и программных средств информационных систем Министерства и учреждений;

2) выхода из строя или невозможность использования линий связи;

3) пожаров, наводнений и других стихийных бедствий, и явлений техногенного характера.

21. Реализация непреднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

1) неумышленных действий, приводящих к частичному или полному нарушению функциональности компонентов информационных систем Министерства и учреждений или разрушению информационных или программно-технических ресурсов;

2) неосторожных действий, приводящих к разглашению информации ограниченного распространения или делающих ее общедоступной;

3) разглашения, передачи или утраты атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т.п.);

4) игнорирования организационных правил при работе с информационными ресурсами;

5) проектирования архитектуры систем, технологий обработки данных, разработки программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем Министерства и учреждений и информационной безопасности;

6) пересылки данных и документов по ошибочному адресу (устройства);

7) ввода ошибочных данных;

8) неумышленной порчи и утраты носителей информации;

9) неумышленного повреждения каналов связи;

10) неправомерного отключения оборудования или изменения режимов работы устройств или программ;

11) заражения компьютеров вирусами;

12) несанкционированного запуска технологических программ, способных вызвать потерю работоспособности информационных систем Министерства и учреждений или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

13) некомпетентного использования, настройки или неправомерного отключения средств защиты.

22. Реализация преднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

1) умышленных действий, приводящих к частичному или полному нарушению функциональности информационных систем Министерства и учреждений или разрушению информационных или программно-технических ресурсов;

2) действий по дезорганизации функционирования информационных систем Министерства и учреждений;

3) хищения документов и носителей информации;

4) несанкционированного копирования документов и носителей информации;

5) умышленного искажения информации, ввода неверных данных;

6) отключения или вывода из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);

7) перехвата данных, передаваемых по каналам связи, и их анализа;

8) хищения производственных отходов (распечаток документов, записей, носителей информации и т.п.);

9) незаконного получения атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);

10) несанкционированного доступа к ресурсам информационных систем Министерства и учреждений с рабочих станций легальных пользователей;

11) хищения или вскрытия шифров криптозащиты информации;

12) внедрения аппаратных и программных закладок с целью скрытного осуществления доступа к информационным ресурсам или дезорганизации функционирования информационных систем Министерства и учреждений;

13) незаконного использования оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;

14) применения подслушивающих устройств, дистанционной фото- и видео съемки для несанкционированного съема информации.

VI. Основные принципы информационной безопасности

23. При построении системы информационной безопасности Министерства и учреждений необходимо руководствоваться следующими основными принципами:

1) законность (осуществление защитных мероприятий и разработки системы информационной безопасности Министерства и учреждений в соответствии с законодательством в области защиты информации);

2) системность (учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности);

3) комплексность (согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов);

4) непрерывность (постоянная работа и организационная поддержка мер и средств защиты для эффективного обеспечения информационной безопасности);

5) своевременность (постановка задач по комплексной защите информации и реализация мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности);

6) преемственность и непрерывность совершенствования (совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и систем их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите);

7) разумная достаточность (выбор достаточного уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми);

8) персональная ответственность (ответственность за обеспечение информационной безопасности для каждого государственного гражданского служащего Министерства и работника учреждения в пределах его полномочий);

9) минимизация полномочий (предоставление пользователям минимальных прав в соответствии с должностными регламентами, должностными инструкциями работников Министерства и учреждений);

10) исключение конфликта интересов (четкое разделение обязанностей работников Министерства и учреждений и исключение ситуаций, когда сфера ответственности допускает конфликт интересов);

11) взаимодействие и сотрудничество (государственные гражданские служащие Министерства и работники и учреждений должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений (ответственных лиц) за обеспечение информационной безопасности);

12) гибкость системы защиты (способность реагировать на изменения внешней среды и условий осуществления Министерства и учреждениями своих функций);

13) простота применения средств защиты (не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при работе

пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций);

14) обоснованность и техническая реализуемость (реализация на современном уровне развития науки и техники, обоснованность с точки зрения достижения заданного уровня безопасности информации, а также соответствие установленным нормам и требованиям по безопасности информации);

15) специализация и профессионализм (реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными работниками);

16) обязательность контроля (обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств).

VII. Меры и средства обеспечения информационной безопасности

24. При осуществлении менеджмента информационной безопасности необходимо выделить следующие основные меры обеспечения информационной безопасности:

1) законодательные (законодательство Российской Федерации в сфере информационной безопасности). Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с государственными гражданскими служащими Министерства и работниками учреждений;

2) морально-этические (нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе). Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в Министерстве и учреждениях;

3) технологические (технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий);

4) организационные (меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность работников, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации);

5) физические (меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для предотвращения несанкционированного доступа к объектам защиты, а также технических средств визуального наблюдения, связи и охранной сигнализации);

6) технические (меры защиты основаны на использовании различных электронных устройств и специального программного обеспечения, выполняющих функции защиты).

25. Для обеспечения информационной безопасности необходимо использовать средства:

1) физической защиты (введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки конфиденциальной информации, оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи);

2) антивирусной защиты (предотвращение потерь, ошибок и модификации информационных ресурсов);

3) резервирования (поддержание целостности и доступности объектов защиты);

4) разграничения доступа (управление доступом к информационным ресурсам, к сети общего пользования, к локальной вычислительной сети);

5) криптографической защиты (защита конфиденциальности, целостности и аутентичности информационных ресурсов путем применения средств криптографической защиты информации, в том числе при передаче по каналам связи);

6) идентификации и аутентификации (предотвращение работы с информационными ресурсами посторонних лиц путем обеспечения возможности распознавания каждого легального пользователя);

7) контроля целостности (своевременное обнаружение модификации или искажения информационных ресурсов, обеспечение правильности функционирования системы защиты и целостности хранимой и обрабатываемой информации);

8) контроля и регистрации событий информационной безопасности (обеспечение обнаружения и регистрации всех событий, которые могут повлечь за собой нарушение информационной безопасности).

26. При выполнении договорных отношений между органами государственной власти Республики Тыва и учреждениями и сторонними организациями (предоставление доступа сторонним организациям к объектам защиты) обязательно выполнение всех необходимых мер и средств обеспечения информационной безопасности.

VIII. Ответственность за нарушение обеспечения информационной безопасности

27. Нарушение информационной безопасности может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.