УТВЕРЖДЕН

приказом государственного
бюджетного учреждения
дополнительного образования
Ставропольского края «Комплексная
спортивная школа»

от 03 сентября 2024 г. № 07-07/79-ОД

ПОЛИТИКА
информационной безопасности ГБУ ДО СК «Комплексная спортивная школа»

1. Общие положения

1.1. Настоящая политика информационной безопасности (далее – политика) определяет цели и принципы обеспечения информационной безопасности в государственном бюджетном учреждении дополнительного образования Ставропольского края «Комплексная спортивная школа» (далее – учреждение).

1.2. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности, достоверности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, достоверность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время, целостность – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению.

1.3. Политика утверждается директором учреждения и обязательна для исполнения всеми сотрудниками учреждения, а также лицами, работающими с информацией, принадлежащей учреждению.

2. Принципы информационной безопасности

2.1. Для информационной безопасности в учреждении соблюдаются следующие принципы информационной безопасности:

- Своевременность обнаружения проблем информационной безопасности. Специалисты учреждения должны своевременно обнаруживать проблемы, потенциально способные повлиять на её безопасность.

- Прогнозируемость развития проблем. Учреждение должно выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.
- Оценка влияния проблем на работу учреждения. Учреждение должно адекватно оценивать степень влияния выявленных проблем.
- Адекватность защитных мер. Учреждение должно выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.
- Эффективность защитных мер. Учреждение должно эффективно реализовывать принятые защитные меры.
- Непрерывность принципов безопасного функционирования. Учреждение должно обеспечивать непрерывность реализации принципов безопасного функционирования.
- Контролируемость защитных мер. Учреждение должно применять только те защитные меры, правильность работы которых может быть проверена, при этом учреждение должно регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на работу учреждения.
- Соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части информационной безопасности.

3. Меры, цели и задачи информационной безопасности

3.1. Меры защиты информации внедряются согласно перечню адаптивного набора мер по обеспечению безопасности информационных систем. Данный перечень определяется по результатам проведения анализа актуальных угроз безопасности информационных систем учреждения, проводимый согласно требованиям законодательства Российской Федерации в области защиты информации. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

3.2. Главной целью принимаемых мер защиты информации учреждения является гарантированное обеспечение целостности, достоверности, доступности и конфиденциальности информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно-вычислительных и телекоммуникационных системах (далее – информационные системы) учреждения независимо от типа носителя этих данных, а также минимизация ущерба от реализации угроз информационной безопасности и улучшение деловой репутации и корпоративной культуры учреждения.

3.3. Организация информационных ресурсов в учреждении должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности учреждения, не жертвуя при этом основными принципами информационной безопасности, описанными в данной политике.

3.4. Информация является важным активом учреждения, и ее защита является обязанностью каждого сотрудника.

3.5. Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

3.6. Для каждого информационного ресурса определяется владелец (Оператор), отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.

3.7. Сотрудники учреждения проходят инструктаж в области информационной безопасности при оформлении на работу, в дальнейшем – с периодичностью, позволяющей специалистам в условиях нарастания количества угроз безопасности информации, а также с учетом необходимости постоянного совершенствования методов и средств их нейтрализации получать новые знания, умения и навыки, необходимые для выполнения должностных обязанностей

3.8. В учреждении регулярно проводится внутренний аудит информационной безопасности согласно плану мероприятий по информационной безопасности, а также возможно проведение независимого аудита.

3.9. Специалист по информационной безопасности учреждения отвечает за определение детальных требований информационной безопасности и контролирует их исполнение в учреждении. На него возлагаются следующие задачи:

- реализация политики в учреждении;
- определение требований к защите информации;
- организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты;
- оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;
- регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;

– в рамках своих полномочий принятие участия в реагировании и расследованиях инцидентов информационной безопасности;

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

3.10. Успешное достижение целей настоящей политики возможно только при выполнении условий и правил следующих детальных положений информационной безопасности учреждения, являющихся приложениями к настоящей политике информационной безопасности ГБУ ДО СК «Комплексная спортивная школа»:

– положение о доступе к информационным ресурсам (приложение 1);

– положение о классификации информации (приложение 2);

– положение по использованию сети Интернет (приложение 3);

– положение по использованию электронной почты (приложение 4);

– положение по использованию парольной защиты информационных ресурсов (приложение 5);

– положение об использовании программного обеспечения (приложение 6);

– положение о защите от вредоносного программного обеспечения (приложение 7);

– положение об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (приложение 8);

– положение о физической защите информационных ресурсов (приложение 9);

– положение по действиям пользователей ИС в нештатных ситуациях (приложение 10).

– перечень сведений конфиденциального характера, обрабатываемых в ГБУ ДО СК «Комплексная спортивная школа» (приложение 11).

3.11. Несоблюдение положений информационной безопасности сотрудниками учреждения может повлечь дисциплинарные меры взыскания вплоть до увольнения на основании действующего законодательства РФ и локальных нормативных актов.