МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

Государственное автономное профессиональное образовательное учреждение Краснодарского края «Брюховецкий многопрофильный техникум»

(ГАПОУ КК БМТ)

УТВЕРЖДЕНО
приказом ГАПОУ КК БМТ
от 10 февраля 2023 г. № 41- ПД

Положение

Об информационной безопасности в государственном автономном профессиональном образовательном учреждении Краснодарского края «Брюховецкий многопрофильный техникум»

I. Общие положения

1.1 Настоящие Положение об информационной безопасности в государственном автономном профессиональном образовательном учреждении Краснодарского края «Брюховецкий многопрофильный техникум» (далее – Положение, техникум) разработано в соответствии с Федеральным законом от 29 декабря 2012 года №273-ФЗ «Об образовании в Российской Федерации, 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», 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», Уставом техникума.

1.2. Информационная безопасность предполагает защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений.

1.3. К субъектам информационных отношений относятся как владельцы, так и пользователи информации и поддерживающей инфраструктуры. К поддерживающей инфраструктуре относятся не только компьютеры, но и

помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и обслуживающий персонал.

1.4. Информационная безопасность в техникуме предусматривает защиту сведений и данных, относящихся к следующим группам:

- персональные данные и сведения, которые имеют отношение к обучающимся, преподавательскому составу, иным категориям работников техникума, оцифрованные архивные документы;

- обучающие программы, базы данных, библиотека, другая структурированная информация, применяемая для обеспечения образовательного процесса;

- защищенная законом интеллектуальная собственность.

1.5. К числу основных направлений обеспечения информационной безопасности относятся:

- правовая защита в виде специальных законов, других нормативных актов, правил, процедур и мероприятий, обеспечивающих защиту информации на правовой основе;

- организационная защита – это регламентация деятельности образовательной организации и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

- инженерно-техническая защита, предполагающая использование различных технических средств, препятствующих нанесению ущерба.

II. Угрозы информационной безопасности

2.1. К числу характерных угроз информационной безопасности относятся не только возможности хищения или повреждения данных хакерами, но также деятельность обучающихся, которые могут сознательно или ненамеренно повредить оборудование или заразить систему вредоносными программами.

2.2. Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

- компьютерное и другое оборудование техникума, в отношении которого возможны воздействия вредоносного программного обеспечения, физические и прочие воздействия;

- программное обеспечение, применяемое в образовательном процессе или для работы системы;

- данные, которые хранятся на жестких дисках или портативных носителях;

- обучающиеся, которые могут подвергаться стороннему информационному воздействию;

- персонал, поддерживающий работу IT-системы.

2.3. Угрозы информационной безопасности в техникуме могут носить непреднамеренный и преднамеренный характер.

2.4. К непреднамеренным угрозам относятся:

- аварии и чрезвычайные ситуации: затопление, отключение электроэнергии и т. д.;

- программные сбои;

- ошибки работников;

- поломки оборудования;

- сбои систем связи.

2.5. Непреднамеренные угрозы могут оказывать лишь временное воздействие и в большинстве случаев должны быстро и эффективно устраняются подготовленным персоналом.

2.6. Наибольшую опасность представляют угрозы информационной безопасности намеренного характера, возникновение которых, невозможно предвидеть.

Намеренные угрозы могут исходить от обучающихся, работников техникума, хакеров. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов, связи между которыми легко нарушаются, что приводит к выведению системы из строя.

2.7. Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав.

2.8. Внешние атаки на компьютерные сети техникума могут предприниматься для воздействия на сознание обучающихся с целью вовлечения их в криминальную или террористическую деятельность.

III. Цели и задачи обеспечения безопасности информации

3.1. Главной целью обеспечения безопасности информации, используемой в техникуме, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды.

3.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, используемой в техникуме;

- предотвращение нарушений прав обучающихся, педагогических работников и других работников техникума на сохранение конфиденциальности информации;

- предотвращение несанкционированных действий по блокированию информации.

3.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам техникума, нарушению его нормального функционирования и развития;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

Э- ффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

- развитие и совершенствование защищенного юридически значимого электронного документооборота;

- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;

- создание механизмов управления системой информационной безопасности.

IV. Механизм обеспечения информационной безопасности

4.1. Техникум самостоятельно определяет состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся и работников. Техникум вправе требовать от своих работников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

4.2. Техникум обязуется обеспечить сохранность конфиденциальной информации.

ПРИНЯТЫ
решением общего собрания техникума
от 03.02.2023 г. протокол № 2