Комитет по образованию
администрации
Ханты-Мансийского района
Ханты-Мансийский
автономный округ - Югра
(Тюменская область)
**Муниципальное автономное учреждение
Ханты-Мансийского района
«Муниципальный методический центр»**
628007, Ханты-Мансийский автономный
округ- Югра, Ханты-Мансийский район,
г. Ханты-Мансийск, ул. Чехова, д.68
Телефон: 8(3467) 32-81-81
E-mail: mmc-hmrn@yandex.ru

ОГРН 1228600004841;
ИНН/КПП 8601072572/860101001

На исх. № от 2024

[Номер документа]
[Дата документа]

Руководителям
общеобразовательных организаций

Уважаемые руководители!

Настоящим направляю информацию по информационной безопасности для применения в работе и размещения на официальных сайтах образовательных организаций.

Информационная безопасность образовательного учреждения представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей. Первой целью является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц. Вторая цель информационной безопасности – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации.

Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

- персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;
- обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;
- защищенная законом интеллектуальная собственность.

Действия злоумышленников могут привести к хищению указанных данных. Также при несанкционированном вмешательстве возможны внесения изменений и уничтожение

хранилищ знаний, программных кодов, оцифрованных книг и пособий, используемых в образовательном процессе.

В обязанности лиц, отвечающих за информационную безопасность, входит:

- обеспечение сохранности защищаемых данных;
- поддержание информации в состоянии постоянной доступности для авторизованных лиц;
- обеспечение конфиденциальности подлежащих защите сведений, предотвращение доступа к ним со стороны третьих лиц.

Спецификой обеспечения информационную безопасность в информационных учреждениях является состав характерных угроз. К ним относится не только возможность хищения или повреждения данных хакерами, но также деятельность учащихся. Подростки могут сознательно или ненамеренно повредит оборудование или заразить систему вредоносными программами.

Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

- компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного ПО, физические и другие воздействия;
- программное обеспечение, применяемое в учебном процессе или для работы системы;
- данные, которые хранятся на жестких дисках или портативных носителях;
- дети и подростки, которые могут подвергаться стороннему информационному воздействию;
- персонал, поддерживающий работу ИТ-системы.

Угрозы информационной безопасности образовательного учреждения могут носить непреднамеренный и преднамеренный характер. К угрозам первого типа относятся:

- аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т. д.;
- программные сбои;
- ошибки работников;
- поломки оборудования;
- сбои систем связи.

Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации предсказуемы, достаточно эффективно и быстро устраняются подготовленным персоналом.

Намного более опасными являются угрозы информационной безопасности намеренного характера. Обычно результаты их реализации невозможно предвидеть. Намеренные угрозы могут исходить от учащихся, персонала организации, конкуренты, хакеры. Лицо, осуществляющее преднамеренное воздействие на компьютерные системы или программное обеспечение, должно быть достаточно компетентным в их работе. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов. Злоумышленники могут достаточно легко нарушать связи между такими удаленными компонентами, что полностью выводит систему из строя.

Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав. Также внешние атаки на компьютерные сети образовательной организации могут предприниматься для воздействия на сознание детей. Наиболее серьезная угроза – возможность вовлечения детей в криминальную или террористическую деятельность.

Современные технологии информационной безопасности образовательной организации предусматривают обеспечение защиты на 5 уровнях:

- нормативно-правовой;

- морально-этический;
- административно-организационный;
- физический;
- технический.

К числу наиболее значимых нормативных правовые актов в области обеспечения информационной безопасности относятся следующие законы и подзаконные акты:

Федеральные законы

1. Федеральный закон от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»
2. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Новая редакция вступила в силу 1 марта 2023 года
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
5. Федеральный закон от 13 марта 2006 г. № 38-ФЗ «О рекламе»
6. Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»
7. Федеральный закон от 27 декабря 2018 г. № 501-ФЗ «Об уполномоченных по правам ребенка в Российской Федерации»
8. Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»
9. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»
10. Федеральный закон от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях»
11. Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации»

Документы стратегического планирования и иные концептуально-программные документы:

1. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации 2 июля 2021 г. № 400)
2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)
3. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента Российской Федерации от 9 мая 2017 г. № 203)
4. Основы государственной политики Российской Федерации в области международной информационной безопасности (утв. Указом Президента Российской Федерации от 12 апреля 2021 г. № 21)
5. Концепция информационной безопасности детей в Российской Федерации (утв. распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р)
6. Стратегия комплексной безопасности детей в Российской Федерации на период до 2030 года (утв. Указом Президента Российской Федерации от 17 мая 2023 г. № 358)
7. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Указом Президента Российской Федерации от 29 мая 2020 г. № 344)

8. Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы (утв. Президентом Российской Федерации 28 декабря 2018 г. № Пр-2665).

Приложение: информационные плакаты в эл.виде.

И.о. директора

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат [Номер сертификата 1]
Владелец [Владелец сертификата 1]
Действителен с [ДатаС 1] по [ДатаПо 1]

И.М. Сперанская

Исполнитель: методист МАУ ХМР «ММЦ»
Софрони Мария Александровна, тел. 8(3467)37-89-69 доб. 205