ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ НАРОДНОГО ОБРАЗОВАНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

О.Ч.Пардаев (ст.пр. Каршинский филиал ТУИТ)

Аннотация. *В статье обсуждается практическое значение информационной безопасности при цифровая тронсформации системы народного образования, проблемы выявления уязвимостей в информационной безопасности и обеспечения ключевых факторов защиты информации от инцидентов информационной безопасности.*

Ключевые слова: *Цифровые технологии, информационная безопасность, народное образование, инциденты, угрозы, меры защиты ИБ.*

ENSURING INFORMATION SECURITY IN THE FIELD OF PUBLIC EDUCATION IN THE CONTEXT OF DIGITAL TRANSFORMATION

O.Ch. Pardaev (Senior Lecturer, Karshi Branch of TUIT)

Abstract. *The article discusses the practical significance of information security in the digital transformation of the public education system, the problems of identifying vulnerabilities in information security, and ensuring key factors for protecting information from information security incidents.*

Keywords: *Digital technologies, information security, public education, incidents, threats, IS protection measures*.

В современном цифровом мире защита информации является критически важным аспектом. Прогнозирование угроз является важным аспектом в области информационной безопасности (ИБ), поскольку позволяет предвидеть потенциальные атаки и принимать меры по их предотвращению.[5] Важным требованием обеспечения деятельности при цифровой тронсформации народного образования является поддержание высокого уровня ИБ. ИБ по мимо защиты баз данных и предотвращения хакерских атак,

важно оградить учащихся от любых проявлений пропаганды и манипуляций. По этому построение системы информационной безопасности в народного образования должны осуществлять специалисты, которые имеют соответствующий уровень квалификации и опыт[1].

ИБ в системе народного 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 ИБ – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации. 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. Спецификой обеспечения ИБ 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:

Рис.1. Уязимости группы объектов.

Для обеспечения мер защиты информационная безопасность при цифровая тронсформации в народного образования, технологии ИБ предусматривают обеспечение защиты на 5 уровнях(рис.2):

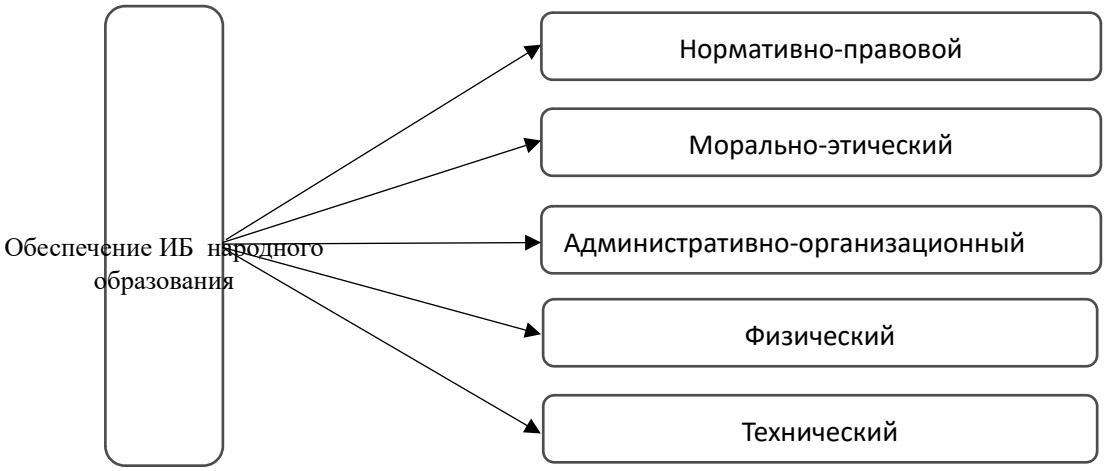

Рис.2. Меры защиты информационной безопасности при цифровой тронсформации народного образования.

1. Нормативно-правовой способ защиты это основным документом, определяющим степень угроз и меры обеспечения информационной безопасности обучающихся в системы народного образования, является «Национальная стратегия действий в интересах детей». Она предусматривает приоритет мер, направленных на защиту сознания ребенка от информационного воздействия агрессивного характера. Меры по защите информационных систем и баз данных имеют второй уровень приоритетности[6].

Законодательством определяются данные, которые должны быть защищены от несанкционированного доступа третьих лиц. К числу таких сведений относятся:

- персональные данные;
- конфиденциальные сведения;
- служебная, профессиональная, коммерческая тайна.

Порядок обеспечения безопасности персональных данных регламентируется Трудовым кодексом, Гражданским кодексом, Законом «Об информации» и другими актами.

Морально-этические средства обеспечения ИБ – это система морально-этических ценностей имеет особое значение в сфере народного образования. Она служит основой для выработки комплекса мер, направленных на защиту детей и подростков от информации этически некорректного, травмирующего, противозаконного характера. В рамках мер по обеспечению ИБ создаются перечни источников (программ, документов и т. д.) способных травмировать детскую психику. В результате принимаемых мер должен предотвращаться доступ таких источников на территорию системы народного образовательного учреждения.

Меры административно-организационного характера - система административно-организационных мер строится на базе внутренних регламентов и правил организации, которыми регламентируется порядок обращения с информацией и ее носителями. В том числе должны быть разработаны:

- должностные инструкции;
- внутренние методики по ИБ;
- перечни не подлежащих передаче данных;
- регламент взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и т. д.

Разработанными методиками должен определяться порядок доступа учеников в интернет во время занятий в компьютерных классах, меры по предотвращению доступа детей к определенным ресурсам, предотвращение использования ими своих носителей информации и т. д.

Физические меры - ответственность за реализацию мер защиты компьютерной сети и носителей информации физического характера несет

непосредственно руководитель образовательной организации и ее IT-персонал. Не допускается перекладывание этих мер на наемные охранные структуры[4].

К числу физических мер относятся:

- реализация пропускной системы для доступа в помещения, в которых находятся носители данных;
- создание системы контроля и управления доступом;
- определение уровней допуска;
- создание правил обязательного регулярного копирования критически важных данных на жесткие диски ПК, не подключенных к интернету.

Технические меры - защиты предусматривают использование специализированного программного обеспечения, которые эффективно обнаруживают угрозы ИБ и обеспечиваю борьбу с ними[4]. При невозможности использования подобных систем по причине бюджетных ограничений, применяются рекомендованные и разрешенные антивирусы и другие виды специального софта. Применяемое для технической защиты программное обеспечение должно обеспечивать контроль электронной почты, которой пользуются ученики или персонал образовательной организации.

Библиографический список

1. Гафнер, В. В. Информационная безопасность. - М.: Феникс,2019**.**
2. Информационная безопасность детей. Российский и зарубежный опыт / Л.Л. Ефимова, А С. А, Кочерга. - М.: Юнити-Дана,2017**.**
3. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - Москва: Высшая школа**,**2019
4. Манако А. Ф. К. М.Синица КТ в обучении: взгляд сквозь призму трансформаций // Образовательные Технологии и Общество. – 2012
5. Бекматов А.К., Кутдусова Э.Р., Мукимов Ш.И., & Давлатова Н.Н. (2023). ПРОГРЕССИВНЫЕ ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО

ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Экономика и социум, (6-1 (109)), 1264-1270.

6. Pardayev O.Ch. (2023). THE ROLE OF THE DIGITAL PLATFORM IN BUSINESS. Экономика и социум, (5-2 (108)), 288-293.