pechatnaya-reklama-vidy-pechatnoj-reklamy.html. – Дата доступа: 27.10.2021.

2. Виды эффективной рекламы [Электронный ресурс] Режим доступа: https://bukivedi.com/blog/vidy-effektivnoy-reklamy/ – Дата доступа: 27.10.2021.

3. Виды рекламной печатной продукции [Электронный ресурс] Режим доступа: https://mediaaid.ru/blog/design/vidy-reklamnoy-pechatnoy-produktsii/#baner. – Дата доступа: 27.10.2021.

4. Виды и особенности применения печатных рекламных материалов [Электронный ресурс] Режим доступа: https:// konstanta-print.ru/news/vidy-i-osobennosti-primeneniya-pechatnykh-reklamnykh-materialov/. – Дата доступа: 27.10.2021.

УДК 621.762.4

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАНИИ

Животкевич Э. Ю.
Научный руководитель: ст. преподаватель Зуёнок А.Ю.
Белорусский национальный технический университет,
г. Минск, Республика Беларусь

В современной литературе существуют дискуссионные понятия кибербезопасности и ее глобальной культуры, киберпространства и безопасного поведения в нем, защиты детей от негативной или вредной информации в информационно-телекоммуникационной сети Интернет.

Кибербезопасность – состояние защищенности киберпространства, сложной среды, создаваемой совокупностью информации, информационной среды и информационного взаимодействия людей.

Информационная безопасность в образовании включает три составляющие: конфиденциальность – защита

чувствительной информации обучающихся и обучающих от несанкционированного доступа; целостность – защита точности и полноты информации и программного обеспечения учебного процесса; доступность – обеспечение доступности информации для познавательного процесса, а также основных информационно-библиотечных и иных услуг для пользователя, несовершеннолетнего обучающегося в том числе, и в нужное для него время: в рамках учебного процесса в образовательной организации или вне ее для индивидуальной работы в домашних условиях.

Во многих странах дети и в особенности подростки часто сталкиваются с кибербуллингом – травлей жертвы через Интернет. Агрессоры действуют через все возможные каналы общения: социальные сети, форумы, чаты, мессенджеры, причиняя жертве серьезные душевные страдания, которые могут привести к психологической травме и/или к суициду.

Осуществлять травлю могут как знакомые жертвы (одноклассники, соседи, интернет-друзья и т. д.), так и совершенно посторонние люди. Так, увидев фотографию жертвы в ИТКС и пользуясь относительной анонимностью Интернета, агрессоры ради развлечения могут затравить ребенка, привлекая к участию в травле себе подобных в интернетсообществах.

Формы травли: нанесение оскорблений через личные сообщения, публикация провокационных материалов, распространение конфиденциальной информации о жертве. Цели: подростковое баловство, получение выгоды, доведение жертвы до самоубийства. Борьба с кибертравлей технически не так проста, поэтому и программный «Родительский контроль» не столь эффективен. При этом дети не способны справиться с агрессорами в одиночку, но зачастую не обращаются к взрослым за помощью, будучи запуганными угрозами, либо просто из-за отсутствия доверия к близким

людям. Отношения с родителями и педагогами играют важную роль в защите ребенка от кибербуллинга.

Педагоги и родители должны помнить об ответственности за безопасность ребенка, не перекладывая ее полностью на программные и технические средства защиты.

Важную роль играет воспитание, подготовка ребенка к информационным угрозам, ведь он никуда не денется от необходимости активного использования информационно-телекоммуникационных сетей.

Таким образом, одна из актуальных задач воспитания обучающихся, состоит в подготовке их к грамотному использованию компьютерных и сетевых технологий, в учебном процессе образовательной организации и вне ее стен, в домашних условиях и в общественных местах с доступом к информационно-телекоммуникационным сетям.

Поэтому сегодня и возникает еще большая потребность в том, чтобы обучающий обладал практическими навыками (новая роль педагога, учителя), зависящими от уровня его познаний, информационной культуры использования ИКТ.

ЛИТЕРАТУРА

1. Международный стандарт ИСО/МЭК 27032: 2012 Руководящие указания по кибербезопасности «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity).

2. Руководство по оценке ИКТ в образовании / Институт статистики Юнеско. – Монреаль, 2011. – 139 с.