Лисневская М. А., студент 308 группы
дневной формы обучения
Научный руководитель – Гончарик Н. Г.,
старший преподаватель

КИБЕРБЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ЗАЩИТЫ

Актуальность данной темы заключается в том, что на сегодняшний день человечество встречается с различными вызовами, которые связаны с глобализацией и научно-техническим процессом. Так, с развитием информационных технологий общество столкнулось с новыми угрозами, происходящими в киберпространстве. Рассматривая в статье кибербезопасность в информационном обществе, киберпространство мы будем понимать как глобальную область информационной среды, включающую в свой состав взаимозависимую совокупность информационно-технической инфраструктуры, в том числе информационные и телекоммуникационные сети и компьютерные системы, предназначенные для хранения, обработки, модификации и обмена данными [1, с. 5]. Безопасность в киберпространстве приобретает первостепенное значение, так как быстрый рост цифровых технологий и повсеместное использование Интернета создают беспрецедентные возможности для киберпреступников. Чтобы не стать жертвой киберпреступников, важно осознавать, что без должной защиты киберпространство может стать уязвимым для кибератак, кражи данных, финансовых мошенничеств и других угроз.

Киберпреступность – быстроразвивающийся вид преступности понимают как следствие глобализации информационно-

коммуникационных технологий и появления международных компьютерных сетей [2, с. 2].

Чтобы разработать систему кибербезопасности, необходимо выделить круг опасностей. Одной из самых актуальных является увеличение количества и сложности кибератак. Киберпреступники постоянно совершенствуют свои методы, используя сложные вредоносные программы и социальную инженерию для кражи данных, вымогательства и других преступных действий. Самой распространенной проблемой, на наш взгляд, является недостаточная осведомленность и неподготовленность пользователей информационного пространства. Многие пользователи не осведомлены о рисках и не принимают надлежащих мер для защиты своих устройств и данных. Отсутствие согласованного подхода – еще одна актуальная проблема информационного общества, что связано с отсутствием глобального сотрудничества и стандартов в области кибербезопасности, что затрудняет борьбу с трансграничными киберугрозами.

Было отмечено большое число актов кибертерроризма на территории Республики Беларусь, потребовавших немедленного реагирования со стороны правоохранительных органов, начиная с 2019 года, когда практически каждый месяц поступали сообщения о минировании зданий по электронной почте [3, с. 326]. С целью результативного сопротивления потребовалась многоуровневая институциональная концепция кибербезопасности, отвечающая за безопасность граждан и государственных институтов.

С одной стороны, для того, чтобы безопасно пользоваться сетью Интернет, нужно соблюдать определенные правила и использовать пути защиты информации, так как защита информации связана с безопасностью. В свою очередь, информационная безопасность – это

обеспечение скрытности, целостности и доступности информации, не ограничивая требований пользования ею [5, с. 569].

Основными методам обеспечения безопасности, и в локальных, и в глобальных сетях, остаются шифрование, идентификация/аутентификация, внедрение физических мер безопасности. Проектирование системы безопасности должно предусмотреть защиту для устройств и шлюзов, сети передачи, а также приложений, которые разворачиваются для обеспечения функционирования устройств [4, с. 43]. Следовательно, с позиции физических мер кибербезопасности речь идет об аппаратно-программном уровне, а на уровне пользователь – это умение использовать

На уровне пользователя регулярное обновление программного обеспечения и операционной системы дает большую гарантию, что компьютер будет защищен актуальными исправлениями безопасности. Использование антивирусных программ – один из самых надежных способов обезопасить свое пребывание в сети Интернет, так как антивирусные программы выявляют и устраняют угрозы, защищая данные от злоумышленников. Одним из известных методов, который применяют киберпреступники, является использование вредоносных ссылок на неизвестные веб-сайты в рассылаемых электронных письмах. К информационной безопасности относится игнорирование таких ссылок и удаление подобного рода писем в категорию спама (нежелательной рассылки). Использование двухфакторной аутентификации повышает безопасность при использовании социальных сетей. Система двухфакторной аутентификации основана на двух «ключах». Первый ключ – это телефон, на который приходит SMS с кодом, второй – это логин и пароль, который нужно запомнить.

Среди киберпреступлений распространен такой феномен, как фишинговое мошенничество. Фишинговые ссылки скрываются под обычные ссылки на веб-сайтах, которые многим кажутся безопасными. При нажатии на вредоносную ссылку учетные данные попадают к мошенникам. Чтобы избежать попадания данных к киберпреступникам, необходимо соблюдать определенные правила. Такие действия, как установление антивирусной программы, проверка адресной строки сайта, с которого пришло сообщение, и избегание оплаты через незнакомые страницы помогут обеспечить безопасность данных. Необходимо внимательно проверять адрес, с которого поступило сообщение, нужно обращать внимание на символы, которые могут отличаться от обычного адреса банка или магазина. При открытии письма необходимо обращать внимание на его написание и оформление. При обнаружении орфографических ошибок и подозрительного дизайна, нужно удалить письмо и не переходить по ссылкам, приложенным в нем.

Таким образом, мы можем сказать, что в современном информационном обществе существует актуальная и важная проблема кибербезопасности, требующая комплексного подхода и постоянного внимания. Понимание и осознание важности кибербезопасности, а также принятие необходимых мер и действий для защиты информации на всех уровнях являются основой для обеспечения стабильной и безопасной работы в цифровом мире. Кибербезопасность требует коллективных усилий со стороны всех участников информационного общества – от индивидуальных пользователей до крупных компаний и государств. Мы должны продолжать развивать и совершенствовать методы защиты, обучать пользователей правилам безопасного поведения в сети,

сотрудничать и делиться информацией о киберугрозах, чтобы сделать информационное пространство более безопасным и надежным.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бородакий, Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Ю. В. Бородакий, И. В. Бутусов, А. Ю. Добродеев // Вопросы кибербезопасности. – 2014. – №1. [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-xxi-veka-chast-2 – Дата доступа : 17.02.2024.

2. Гундерич, Г. А. Состояние киберпреступности / Г. А. Гундерич // Научный вестник Крыма. – 2018. – №4. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti – Дата доступа : 17.02.2024.

3. Декола, И. В. Проблема обеспечения кибербезопасности в Белоруссии, России и Украине / И. В. Декола, Б. Э. Петрашко, А. Д. Магомедова // Постсоветские исследования. – 2020. – №4. [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/problema-obespecheniya-kiberbezopasnosti-v-belorussii-rossii-i-ukraine – Дата доступа : 15.02.2024.

4. Полегенько, М. А. Особенности защиты информации в Интернете вещей / М. А. Полегенько // International Journal of Open Information Technologies. – 2018. – №10. [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/osobennosti-zaschity-informatsii-v-internete-veschey – Дата доступа : 16.02.2024.

5. Мавлянова, Л. Т. Защита информации в Интернет / Л. Т. Мавлянова // Постсоветские исследования. – 2022. – №1. [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/zaschita-informatsii-v-internet – Дата доступа : 17.02.2024.

Лозюк К. С., студент 114Р группы
дневной формы обучения
Научный руководитель – Котович О. В.,
кандидат культурологии, доцент

«ТЕАТР ДЭЛЬ АРТЕ» КАК ОДИН ИЗ ЖАНРОВ СРЕДНЕВЕКОВЫХ ТЕАТРАЛИЗОВАННЫХ ПРЕДСТАВЛЕНИЙ

Комедия Дель Арте – итальянская комедия масок, которая строится на импровизационных постановках под открытым небом и устойчивых персонажах (масках). Данный вид представлений возник благодаря карнавалам и уличным представлениям еще в середине 16 века. Считается, что впервые упоминание о комедии масок берет истоки из северо-востока Италии в 1545 г. Позже, к 1550-м г. появляются первые упоминания о представлениях с участием масок.

Углубившись в историю средневековой культуры, следует отметить, народная комедия Дель Арте усиленно изучалась в 20 веке в СССР такими исследователями как Г.Н. Бояджиев, А.К. Дживелегов, С. С. Мокульский и др.

На современном этапе следует отметить таких исследователей как Д. В. Трубочкин и М. М. Молодцова.