Список литературы

1. *Кужелева-Саган Д.И.* Спичева феномен цифрового кочевничества в современном междисциплинарном дискурсе. Режим доступа: https://cyberleninka.ru/article/n/fenomen-tsifrovogo-kochevnichestva-v-sovremennom-mezhdistsiplinarnom-diskurse/viewer

2. Мобильные метафоры туристы и кочевники Дж. Урри. Режим доступа: https://cyberleninka.ru/article/n/fenomen-tsifrovogo-kochevnichestva-v-sovremennom-mezhdistsiplinarnom-diskurse/viewer

3. *Прогноз* PwC на основании данных Askwonder // What is the Global market-size (TAM) for the Gig-Freelancer Economy industry

4. *Родиченков Ю.Ф.* Двадцать веков алхимии: от псевдо-Демокрита до наших дней // РХГА. 2019. С. 94-95.

5. Стратегия 2050. Обзорно-аналитический портал. Режим доступа: https://strategy2050.kz/ru/news/internet-v-selakh-plany-sroki-i-realizatsiya

6. *Зигмунт Б.* Текучая современность. Режим доступа: https://cyberleninka.ru/article/n/fenomen-tsifrovogo-kochevnichestva-v-sovremennom-mezhdistsiplinarnom-diskurse/viewer

УДК 336

Д.Н. Маматов, Ш.Б. Бекчонова
D.N. Mamatov, Sh.B. Bekchonova
Ташкентский государственный педагогический университет
Ташкент, Узбекистан
Tashkent State Pedagogical University
Tashkent, Uzbekistan
bshb79@mail.ru

ПЕДАГОГИЧЕСКИЕ РЕШЕНИЯ ПО ПРЕДОТВРАЩЕНИЮ РАЗВИТИЯ КИБЕРАТАК
PEDAGOGICAL SOLUTIONS TO PREVENT THE DEVELOPMENT OF CYBER ATTACKS

Аннотация. В статье обсуждается, как кибербезопасность может быть защищена от кибератак в 21 веке путем обучения студентов цифровой грамотности.

Annotation. The article discusses how cybersecurity can be protected from cyber attacks in the 21st century by teaching digital literacy to students.

Ключевые слова: кибератака, кибербезопасность, педагогический подход, цифровая грамотность, программное обеспечение.

Keywords: cyber attack, cyber security, pedagogical approach, digital literacy, software.

Возрастающую актуальность информационной безопасности можно объяснить тем, что информация становится стратегическим ресурсом. Современная государственная инфраструктура состоит из телекоммуникационных и информационных сетей и различных информационных систем, а информационные технологии и технические средства широко используются в различных сферах жизни общества (экономика, наука, образование, военное дело, управление различными технологиями и др.). Глобальные проблемы нашего века уже давно характеризуются появлением киберпреступности, которая упоминается в новых формах. Его распространением известных вирусных программ, взломом паролей, хищением средств на кредитных картах и других банковских реквизитах, а также нелегальной информацией в сети Интернет, в частности клеветой, морально мы не можем игнорировать тот факт, что распространение недостоверной информации представляет собой большую угроза жизни человека [1].

Понятие «киберпреступность» включает в себя использование информационно-коммуникационных технологий для устрашения виртуальной сети, вирусов и других вредоносных программ, подготовку и распространение нелегальной информации, массовую рассылку электронных писем (спама), взлом, незаконный доступ к веб-сайтам, мошенничество, целостность данных и нарушение авторских прав, номер кредитной карты и кража банковских реквизитов (фишинг и фарминг) и различные другие нарушения.

Следует отметить, что масштабы кибертерроризма и его угроза общественной жизни растут. Кибертеррористический акт (кибератака) - причинение ущерба материальным объектам в крупном размере, совершенное с помощью средств вычислительной техники и информационно-коммуникационных средств, создающее прямую или потенциальную угрозу жизни и здоровью людей. начало или цель общественно опасных последствий, которые могут возникнуть. Привлекательность использования киберпространства для современных террористов обусловлена тем, что осуществление кибератаки не требует больших финансовых затрат.На данный момент кибербезопасность может показаться простым термином, который с практической точки зрения имеет совершенно разные значения для разных людей в разных ситуациях и приводит к различным соответствующим политикам, процедурам и практикам. Любой, кто хочет защитить свои учетные записи в социальных сетях от хакерских атак, скорее всего, будет использовать подходы и технологии кибербезопасности, используемые, например, многими пользователями компьютеров для защиты секретных сетей [2].

Обычно под кибербезопасностью понимают:

Для физических лиц кибербезопасность означает, что их личная информация недоступна никому, кроме них самих и лиц, обладающих такими полномочиями, и что их компьютеры работают должным образом и не содержат вредоносных программ. Для отдельного владельца малого бизнеса кибербезопасность может включать в себя обеспечение надлежащей защиты информации о кредитной карте и надлежащего соблюдения стандартов безопасности данных в реестрах торговых точек. Фирмы, которые занимаются онлайн-бизнесом для физических лиц, включают в себя защиту серверов, которые постоянно работают с доверенными серверами, включая кибербезопасность. Для поставщиков общих услуг кибербезопасность сюда входят несколько центров обработки данных, в том числе большое количество серверов с несколькими виртуальными серверами, принадлежащими многим различным организациям, может потребоваться защита. Для правительства кибербезопасность может включать определение различных классификаций, каждая из которых имеет свой набор законов, политик, процедур и технологий.

Чтобы решить эти проблемы, наука о новых основах кибербезопасности объясняет основы безопасности, включая принципы безопасности, критические элементы управления безопасностью и лучшие практики кибербезопасности. Студенты также оценят управление системой, которое соответствует отраслевым стандартам и ключевым элементам управления, специальные методы безопасности, используемые для оценки высокоуровневых рисков, уязвимостей и векторов атак типичной системы, и объяснят, как устанавливать и обслуживать различные типы компьютеров.

В области кибербезопасности мы можем увидеть много практического опыта и исследований ученых и педагогов. Вот несколько примеров:

Исследования Microsoft: основные достижения в области безопасности для служб, включая алгоритмы обнаружения десятков миллионов вредоносных учетных записей электронной почты. Государственные и частные исследователи создали операционную систему Linux с улучшенной безопасностью. Исследования в Google могут помочь улучшить такие продукты, как безопасность браузера Chrome и отпечатки видео на YouTube. Компания Symantic research labs внедряет новые алгоритмы для компании, увеличивает скорость работы и внедряет продукты. Кибербезопасность - это практическая наука. То есть преподаватели и учащиеся в этой области часто используют факты и научные открытия, известные в виде цифровых технологий, для создания полезных приложений. Кибербезопасность используется и в других областях науки, например, в естественных науках (биология), формальных науках (статистика) и социальных науках (экономика). Можно с уверенностью сказать, что кибербезопасность совместима с интеграцией всех дисциплин в развитие системы образования. И на это влияют отношения с социальными науками, такими как экономика, социология и криминология.

Также принимать необходимые решения по выявлению, устранению и предупреждению киберпреступлений и участвовать в разработке проектов нормативных актов по борьбе с киберпреступностью, по выявлению и противодействию киберугрозам, угрожающим интересам государственных органов и кибербезопасности. Необходимо обучать людей, разбирающихся в этой области, и обучать их цифровой грамотности, выявлять и устранять

причины и условия, позволяющие киберпреступности угрожать правам и свободам граждан. Наши современные педагоги продвигаются в XXI веке по таким вопросам. Они постоянно учатся и преподают соответствующие программы, потому что у нас светлое будущее, а кибератаки можно предотвратить, повышая цифровую грамотность следующего поколения.

Список литературы

1. *Мельников В.Н., Клейменов С.А.* Информационная безопасность и защиты информации. Москва 2008.236 с.

2. *Тураев Б.А.* Криптографическая защита электронного документооборота.Ташкент 2015. 213 с.

УДК 336.6

М.В. Денисова, А.В. Ефанов
M.V. Denisova, A.V. Efanov
Российский государственный профессионально-педагогический университет
Екатеринбург, Россия
Russian State Vocational Pedagogical University
Yekaterinburg, Russia
dnsva.ma@gmail.com

АНАЛИЗ ПЕРСПЕКТИВ И ТЕНДЕНЦИЙ РАЗВИТИЯ ЭЛЕКТРОННОЙ КОММЕРЦИИ НА ПРИМЕРЕ ТОРГОВОЙ ПЛОЩАДКИ «WILDBERRIES»
ANALYSIS OF PROSPECTS AND TRENDS IN THE DEVELOPMENT OF E-COMMERCE ON THE EXAMPLE OF THE TRADING SITE «WILDBERRIES»

Аннотация. В условиях развития информационного общества люди общаются, работают, совершают сделки, покупки с помощью сети Интернет. Интернет из технологической сети специального назначения трансформировался в экономическую, став средой взаимодействия для агентов рынка.

Annotation. In the conditions of the development of the information society, people communicate, work, make transactions, purchases using the Internet. The Internet has been transformed from a special-purpose technological network into an economic one, becoming an interaction environment for market agents.

Ключевые слова: электронная коммерция, интернет-магазины, маркетплейс, Wildberries, Интернет и общество, информационные технологии, тренды.

Keywords: e-commerce, online stores, marketplace, Wildberries, Internet and society, information technology, trends.

В данный момент, на экономику оказывает воздействие два важнейших процесса современности: цифровизации и глобализации. Цифровизация оказывает все большее влияние на все сферы экономики. В последние годы высокие темпы роста демонстрирует онлайн-торговля. Коммерческую деятельность в сети Интернет, на данный момент, можно назвать достаточно «свежим» направлением розничной торговли. Наблюдается тренд к повсеместности внедрения и использования информационных технологий, а также формирования глобального, но дешёвого бизнеса, помогающего экономить как деньги, так и времени покупателей. Эти тренды плавно задают направление развития электронной коммерческой деятельности и появлению целых интернет-компаний.

Можно выделить основные факторы, повлиявшие на рост объема интернет-торговли за последнее время:

продолжительное количество нерабочих дней с сохранением заработной платы во время карантина способствовало привлечению потока покупателей в интернет-магазины, многие из которых впоследствии останутся и будут делать покупки через интернет;

введение формата удаленной работы. У покупателей появилась возможность, не отрываясь от рабочего процесса делать покупки, сократить количество поездок и отдалиться от центров традиционной торговли;

ограничение количества перемещений в магазины и жесткий контроль за соблюдением санитарных правил;

достаточный уровень развития интернет-магазинов, логистики, для обеспечения товаром каждого покупателя в любой точке страны;