МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кузбасский государственный технический университет имени т. Ф. Горбачёва»
Филиал КузГТУ в г. Новокузнецке,
Башкирский кооперативный институт (филиал) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации
«Российский университет кооперации»

при участии филиала Российского общества «Знание» в Кемеровской области-Кузбассе

VII Международная научно-практическая конференция, приуроченная к Году педагога и наставника

ВОПРОСЫ СОВРЕМЕННОЙ НАУКИ: ПРОБЛЕМЫ, ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

8 декабря 2023 года

Кемерово
2023

УДК 001.12
ББК 70
В 74

Печатается по решению Учёного совета
Филиала КузГТУ в г. Новокузнецке

В74 Вопросы современной науки: проблемы, тенденции и перспективы (Год педагога и наставника): материалы VII международной научно-практической конференции, г. Новокузнецк, 8 декабря 2023 г. (часть 2) / отв. ред. Т.А. Евсина; ред. кол. канд. экон. наук Ю.А. Кузнецова [и др.]. – Кемерово: ФГБОУ ВО «Кузбасский государственный технический университет им. Т.Ф. Горбачева», филиал КузГТУ в г. Новокузнецке, 2023. – 216 с. ISBN 978-5-00137-433-6

В настоящий сборник вошли материалы участников VII международной научно-практической конференции «Вопросы современной науки: проблемы, тенденции и перспективы (Год педагога и наставника)». Авторы рассматривают актуальные проблемы и перспективы системы образования страны, задачи популяризации науки и развитие просветительской деятельности в России, возможности сохранения и повышения профессионализма педагога в информационном обществе, возможности и достижения в области техники и технологии в России, роль социально-гуманитарных наук в социально-экономическом развитии страны, особенности формирования и перспективы развития современной экономики России, а также проблемы противодействия угрозам в современном мире.

Авторами материалов конференции предлагаются научно-обоснованные теоретико-методологические подходы и даются конкретные рекомендации, предназначенные для решения актуальных вопросов в сфере производства, науки и образования.

ISBN 978-5-00137-433-6

И можно сказать больше. Фраза, сказанная Магомедом Нурбагандовым, не осталась только в Дагестане, а пошла по всей стране. Я уверен, что каждый из нас слышал ее до сегодняшнего дня.

Наклейки с Героем России Магомедом Нурбагандовым и его фразой сейчас можно увидеть на служебных машинах сотрудников полиции, на танках и нашивках в Сирии, где военнослужащие продолжают противостоять терроризму на мировом уровне, а так же на военной технике, находящейся в зоне СВО, где военные борются с неонацизмом и неофашизмом.

Таким образом, можно сделать вывод, что такие качества личности, как мужество и героизм являются фактором противодействия процесса виктимизации в условиях криминального конфликта.

Список источников

1) Варчук Т.В., Вишневецкий К.В. Виктимология. – М., 2008.– С.191.
2) Криминология. Курс лекций/Под ред. проф. З.А.Астемирова. – Махачкала, 2002. – С.125.

УДК 004.056.57

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ КИБЕРАТАК

Керимова А.И.
Организация перевозок на железнодорожном транспорте, 1 курс
Ионина А.В.[2]
Кандидат технических наук, доцент, заведующий кафедрой ТДиИТ
[1]Сибирский государственный индустриальный университет, г. Новокузнецк
[2]Филиал «Кузбасский государственный технический университет имени Т.Ф. Горбачева» в г. Новокузнецке, г. Новокузнецк
e-mail: ani-vo@yandex.ru

Аннотация: Современные угрозы кибератак представляют собой серьёзные вызовы информационной безопасности. Для эффективного противодействия этим угрозам необходимо решить несколько ключевых задач, которые рассмотрены в данной статье.
Ключевые слова: кибератаки, киберграмотность, IT технологии, информация, информационные технологии, уязвимости, веб-сервер, скриптинг.

Стремительное развитие технологий в современном мире открывает множество возможностей для повышения качества жизни, экономического развития и научных исследований. Следовательно, и угрозы не стоят на месте, а постоянно развиваются, что делает сложной задачу постоянного обновления систем безопасности. Организациям часто не хватает времени на адаптацию мер киберзащиты к новым видам угроз [1]. Отметим некоторые ключевые аспекты:

– *технологический процесс:* подключение к сети всех типов устройств (от «умных домов» до промышленных систем) увеличивает количество точек входа для потенциальных кибератак;

– *новые точки входа для кибератак:* передовые алгоритмы и системы искусственного интеллекта могут использоваться как для защиты, так и для нападения. Например, атаки на основе машинного обучения могут стать более изощрёнными и труднообнаружимыми.

– *кибератаки* становятся все более изощренными и масштабными. Например, киберпреступники могут атаковать государственные учреждения, критически важные объекты инфраструктуры или предприятия.

– *ransomware и кибервымогательство:* киберпреступники все чаще используют программы ransomware для шифрования данных, а потом требуют выкуп за их восстановление. По сути – сетевой червь, самостоятельно распространяющийся в интернете

и в локальных сетях через уязвимости в ПО, особенно в MicrosoftWindows. Кибератаки могут угрожать организациям, государствам и даже отдельным лицам в разных частях света [2].

Если рассмотреть процентное соотношение последствий кибератак для компаний, можно сделать вывод, что утечка информации – это основная цель кибератак и составляет 58 %, в то время как нарушение технологического процесса находится на последнем месте и составляет всего лишь 20%.

Рисунок 1– Процентное соотношение последствий кибератак

Социальная инженерия и фишинговые атаки могут полагаться на ошибку или невнимательность пользователя для обхода технических средств защиты. И, как следствие, наносят неустранимые уязвимости, которые могут быть использованы злоумышленниками. В 2022 году зафиксировали 7 типов кибератак [3,4]:

1. Атаки типа отказ в обслуживании – являются основным видом атак, применяемых сегодня, и направленных в первую очередь на вывод систем из строя или маскировку других видов кибератак.

2. Deface характеризуется заменой содержимого нарушенного информационного ресурса и размещением на нем вызывающего сообщения с целью пропаганды и нанесения репутационного ущерба владельцу сайта.

3. Фишинговые письма – это вид интернет-мошенничества, основанный на методах социальной инженерии, целью которого является психологическое манипулирование людьми с целью заставить их совершить определенные действия или разгласить конфедициальную информацию.

4. Вредоносные программные инъекции – внедрение MSI в информационные системы различных организаций с целью проникновения в их инфраструктуру или выполнения деструктивных действий (например, шифрования данных), направленных на IT-инфраструктуру.

5. Брутфорс к сервисам удалённого доступа – суть подхода заключается в последовательном автоматическом переборе всех возможных комбинаций символов для поиска правильной комбинации имени пользователя и пароля.

6. Автоматизированное сканирование информационных ресурсов с целью обнаружения критических уязвимостей и неправильно настроенного программного

обеспечения на периметре сети организации, которые могут быть использованы хакерами для проникновения в инфраструктуру и компрометации данных и информационных систем.

7. Выполнение произвольного кода на веб-сервере. Примерами могут служить SQL – инъекции и межсайтовый скриптинг. Эти атаки позволяют получить доступ к базам данных или внедрить вредоносный код в веб-системы.

Следовательно, можно сделать вывод, что для того, чтобы сократить вероятность кибератак нужно соблюдать элементарные меры безопасности и профилактики: для повышения безопасности доступа может быть добавлена многофакторная аутентификация; регулярные обновления позволяют устранить уязвимости системы; поддерживать навыки и знания сотрудников в актуальном состоянии и следить за последними изменениями в области кибербезопасности; ввести чёткую организационную политику безопасности и обеспечить её соблюдение всеми сотрудниками.

Обеспечение высокого уровня киберграмотности персонала является ключевым элементом успешной работы в цифровой среде, защищающим от таких угроз. Для снижения угрозы кибератак и обеспечения общей безопасности важно сочетание технических, организационных и человеческих мер защиты.

Список источников

1) Крутова, Н. А. Проблема управления кибербезопасностью в целях стабилизации развития экономики России на современном этапе / Н. А. Крутова, А. Н. Крутов, Т. М. Тарасова // Вестник СамГУПС. – 2022. – № 3(57). – С. 73-82.

2) Рожнов, Д. А. Информатика и проблемы кибербезопасности / Д. А. Рожнов, А. В. Ионина // Вопросы современной науки: проблемы, тенденции и перспективы (современный мир в условиях глобальной турбулентности): Материалы VI Международной научно-практической конференции, Новокузнецк, 08–09 декабря 2022 года / Отв. редактор Т.А. Евсина редколлегия: Ю.А. Кузнецова [и др.]. – Кемерово-Новокузнецк: Кузбасский государственный технический университет имени Т.Ф. Горбачева, филиал КузГТУ в г. Новкузнецке, 2022. – С. 153-154. – EDN DMQBWG.

3) Кодзокова, Л. А. Проблемы противодействия киберпреступности в Российской Федерации / Л. А. Кодзокова // Пробелы в российском законодательстве. – 2023. – Т. 16, № 4. – С. 287-292.

4) Ржевская, Н. В. Исследование актуальных угроз международной информационной безопасности / Н. В. Ржевская, В. С. Пелешенко, Ю. А. Андрусенко // Студенческая наука - для развития информационного общества: Сборник научных трудов по материалам XIV Всероссийской научно-технической конференции, Ставрополь, 18 мая 2023 года. – Ставрополь: Северо-Кавказский федеральный университет, 2023. – С. 60-64.

УДК 323.2

К ВОПРОСУ О РЕАЛИЗАЦИИ ПОЛИТИКИ ПАМЯТИ

Колыганова В.А., Строительство, 08.03.01, 1 курс
e-mail: wiktoory@gmail.com
Валиева А.Р., кандидат политических наук, доцент кафедры социально-экономических и гуманитарных дисциплин
ФГБОУ ВО «Башкирский государственный аграрный университет», Уфа
e-mail: valieva.ar@rambler.ru

Аннотация. В статье рассматривается политика памяти как самостоятельное направление государственной политики. Раскрывается необходимость формирования и реализации политики памяти и исторической политики в нашей стране, особенно среди молодежи. Авторы описывают методы осуществления данной политики на федеральном и региональном уровнях.

Ключевые слова. Политика памяти, государственная политика, патриотизм.