International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

КИБЕРРЕЗИЛИЕНЦИЯ И МАКРОЭКОНОМИЧЕСКАЯ УСТОЙЧИВОСТЬ: ВЗАИМОДЕЙСТВИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЭКОНОМИЧЕСКИХ СИСТЕМ

https://doi.org/10.5281/zenodo.11081759

Карабаев Рустам Зафарович
Ташкентский университет информационных технологий,
студент 3 курса факультета экономики и менеджмента в сфере ИКТ
Саиткамолов Мухаммадхожа Сабирходжа угли
Ташкентский университет информационных технологий,
Декан факультета экономики и менеджмента в сфере ИКТ,
доктор экономических наук

Аннотация

С ростом зависимости экономических систем от информационных технологий и цифровых сетей, угрозы кибербезопасности становятся все более значимыми. Кибератаки, хакерские атаки и другие формы киберугроз могут иметь серьезные последствия для экономических систем, включая прерывание бизнес-процессов, утечку конфиденциальной информации и нарушение доверия клиентов. Статья исследует, как киберрезилиенция - способность экономических систем справляться с кибератаками и быстро восстанавливать свою работоспособность - связана с общей макроэкономической устойчивостью. Она обсуждает важность принятия мер по обеспечению информационной безопасности на уровне государственной политики, регуляторных органов и предприятий.

Ключевые слова

информационные технологии, цифровые сети, угрозы кибербезопасности, кибератаки, киберугрозы, экономические системы, бизнес-процессы, конфиденциальная информация, киберрезилиенция, макроэкономическая устойчивость.

KIBERREZILIYENSIYA VA MAKROIQTISODIY BARQARORLIK: AXBOROT XAVFSIZLIGI VA IQTISODIY TIZIMLARNING O'ZARO TA'SIRI

Karabayev Rustam Zafarovich
Toshkent axborot texnologiyalari universiteti,
AKT sohasida iqtisodiyot va menejment fakulteti yo‘nalishi bo‘yicha 3-kurs talabasi
Saitkamolov Muxammadxo‘ja Sobirxo‘ja o‘g‘li

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

Toshkent axborot texnologiyalari universiteti,
AKT sohasida iqtisodiyot va menejment fakulteti dekani,
Iqtisodiyot Fanlari Doktori

Annotatsiya

Iqtisodiy tizimlarning axborot texnologiyalari va raqamli tarmoqlarga bog'liqligi ortib borayotganligi sababli, kiberxavfsizlik tahdidlari tobora muhim ahamiyat kasb etmoqda. Kiberhujumlar, xakerlik hujumlari va kiber tahdidlarning boshqa shakllari iqtisodiy tizimlarga jiddiy ta'sir ko'rsatishi mumkin, shu jumladan biznes jarayonlarining uzilishi, maxfiy ma'lumotlarning tarqalishi va mijozlar ishonchining buzilishi. Maqolada kiberreziliyensiya - iqtisodiy tizimlarning kiberhujumlarga qarshi kurashish va ularning ish faoliyatini tezda tiklash qobiliyati - umumiy makroiqtisodiy barqarorlik bilan qanday bog'liqligi ko'rib chiqiladi. U davlat siyosati, tartibga solish organlari va korxonalar darajasida axborot xavfsizligini ta'minlash choralarini ko'rish muhimligini muhokama qiladi.

Kalit so'zlar

axborot texnologiyalari, raqamli tarmoqlar, kiberxavfsizlik tahdidlari, kiberhujumlar, kiber tahdidlar, iqtisodiy tizimlar, biznes jarayonlari, maxfiy ma'lumotlar, kiberreziliyensiya, makroiqtisodiy barqarorlik.

CYBERRESISTANCE AND MACROECONOMIC STABILITY: THE INTERACTION OF INFORMATION SECURITY AND ECONOMIC SYSTEMS

Karabaev Rustam Zafarovich
Tashkent University of Information Technologies,
3rd year student of the Faculty of Economics and Management in the Field of ICT
Saitkamolov Mukhammadkhoja Sabirkhoja ugli
Tashkent University of Information Technologies,
Dean of the Faculty of Economics and Management in the Field of ICT,
Doctor of Economic Sciences

Annotation

With the increasing dependence of economic systems on information technology and digital networks, cybersecurity threats are becoming increasingly significant. Cyberattacks, hacker attacks and other forms of cyber threats can have serious consequences for economic systems, including interrupting business processes, leaking confidential information and violating customer trust. The article explores how cyberresistance - the ability of economic systems to cope with cyber-attacks and quickly restore their efficiency - is related to overall

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

macroeconomic stability. She discusses the importance of taking measures to ensure information security at the level of government policy, regulatory authorities and enterprises.

Keywords

information technologies, digital networks, cybersecurity threats, cyber-attacks, cyber threats, economic systems, business processes, confidential information, cyberresistance, macroeconomic stability.

Введение. В современной цифровой эпохе, когда экономика все больше зависит от информационных технологий и цифровых систем, обеспечение информационной безопасности становится неотъемлемым компонентом обеспечения макроэкономической устойчивости. Эта статья исследует взаимосвязь между киберрезилиенцией, т.е. способностью системы справляться с кибератаками и быстро восстанавливать свою работоспособность, и макроэкономической устойчивостью.

Методология исследования. Статья анализирует, как киберугрозы и кибератаки могут оказывать негативное влияние на экономические системы, включая прерывание бизнес-процессов, утечку конфиденциальной информации, финансовые потери и снижение доверия со стороны клиентов и партнеров. Она также обсуждает, как макроэкономическая устойчивость может быть подорвана в результате кибератак и как эта проблема становится все более актуальной в контексте современной цифровой экономики. Статья предлагает стратегии и подходы для повышения киберрезилиенции экономических систем. Это включает разработку и реализацию превентивных мер, таких как улучшение информационной безопасности, обучение персонала, разработка планов реагирования на происшествия и восстановления после атаки. Она также рассматривает важность сотрудничества между государственными органами, частным сектором и академическими институтами для эффективной борьбы с киберугрозами и обеспечения устойчивости экономических систем.

Литературный обзор. В последние годы отношение между информационной безопасностью и макроэкономической устойчивостью привлекает все больше внимания исследователей. Концепция киберрезилиенции, определяемая как способность системы справиться с кибератаками и быстро восстановить свою работоспособность, становится ключевым аспектом обеспечения устойчивости экономических систем в цифровую эпоху. В работе "Киберрезилиенция и макроэкономическая

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

устойчивость: взаимодействие информационной безопасности и экономических систем" авторы (исследователи) рассматривают различные аспекты этой проблематики и предлагают перспективы для дальнейших исследований. В рамках обзора литературы, авторы провели анализ существующих исследований и публикаций, связанных с киберрезилиенцией и ее влиянием на макроэкономическую устойчивость. Одним из основных выводов обзора является то, что киберугрозы и кибератаки могут иметь серьезные последствия для экономических систем. Прерывание бизнес-процессов, утечка конфиденциальной информации, финансовые потери и снижение доверия клиентов - все это факторы, способные подорвать макроэкономическую устойчивость. Киберрезилиенция становится важным аспектом стратегий и мер, направленных на обеспечение устойчивости экономических систем в условиях цифровой экономики.

Результаты исследования. Взаимосвязь киберрезилиенции и макроэкономической устойчивости становится все более очевидной в современном мире, где информационные технологии (ИТ) играют все более важную роль в функционировании экономических систем. Кибератаки могут нанести значительный ущерб экономике, нарушив работу критической инфраструктуры, приведя к краже конфиденциальных данных и финансовым потерям. Киберрезилиенция - это способность системы противостоять кибератакам, минимизировать ущерб от них и быстро восстанавливаться после них. Она является важным фактором макроэкономической устойчивости, поскольку может помочь защитить экономику от негативных последствий киберугроз.

Существует несколько каналов, через которые киберрезилиенция может влиять на макроэкономическую устойчивость:

- **Прямой канал:** Кибератаки могут напрямую нанести ущерб экономике, нарушив работу критической инфраструктуры, приведя к краже конфиденциальных данных и финансовым потерям.
- **Косвенный канал:** Кибератаки могут подорвать доверие к экономике, что может привести к снижению инвестиций, росту процентных ставок и замедлению экономического роста.
- **Системный канал:** Кибератаки могут иметь каскадный эффект, когда одна атака приводит к другим атакам, что может привести к системному кризису.

Существует ряд мер, которые правительства, предприятия и отдельные лица могут предпринять для повышения киберрезилиенции:

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

1) На уровне правительства:

- Разработка и реализация национальной стратегии кибербезопасности;
- Создание и финансирование программ по повышению осведомленности о кибербезопасности;
- Поддержка исследований и разработок в области кибербезопасности;
- Сотрудничество с другими странами по вопросам кибербезопасности.

2) На уровне предприятия:

- Внедрение надежных мер кибербезопасности, таких как брандмауэры, антивирусное программное обеспечение и шифрование;
- Регулярное обучение сотрудников вопросам кибербезопасности;
- Разработка и реализация плана реагирования на киберинциденты;
- Страхование от киберрисков.

3)На уровне отдельных лиц:

- Использование надежных паролей и хранение их в секрете;
- Установка обновлений программного обеспечения;
- Осторожность при открытии вложений электронной почты и переходе по ссылкам;
- Использование надежных антивирусных и антишпионских программ.

Повышение киберрезилиенции является важной задачей для всех заинтересованных сторон. Это поможет защитить экономику от негативных последствий киберугроз и способствует созданию более устойчивой и процветающей экономики. В дополнение к вышесказанному, важно отметить, что киберрезилиенция не является статичным понятием. Она должна постоянно развиваться и адаптироваться к новым киберугрозам. Необходимо постоянно следить за новыми угрозами и уязвимостями, а также разрабатывать новые методы их защиты.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

Рис.1 Структура методологии анализа эффективности вложений в проекты по обеспечению информационной безопасности [1]

Структура методологии анализа эффективности вложений в проекты по обеспечению информационной безопасности может включать следующие составляющие:

1. Определение целей и задач:

a) Определение основных целей и задач проектов по обеспечению информационной безопасности.

b) Установление приоритетов и адекватного бюджета для каждого проекта.

2. Оценка угроз и рисков:

a) Проведение анализа угроз информационной безопасности, связанных с организацией или системой.

b) Оценка вероятности возникновения угроз и потенциальных негативных последствий.

c) Идентификация критических активов и уязвимостей.

3. Определение требуемого уровня безопасности:

a) Установление необходимого уровня защиты информации и безопасности системы.

b) Определение соответствующих стандартов и нормативов, которым должна удовлетворять система.

4. Разработка плана проекта:

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

a) Разработка детального плана действий для каждого проекта, включая распределение ресурсов, временные рамки и ответственность.

b) Определение ключевых этапов и достижимых результатов.

5. Оценка затрат:

a) Оценка затрат, связанных с реализацией проектов по обеспечению информационной безопасности.

b) Учет расходов на приобретение и внедрение технических средств, обучение персонала, поддержку и обновление системы.

6. Оценка преимуществ и рисков:

a) Оценка ожидаемых преимуществ и выгод от реализации проектов по обеспечению информационной безопасности.

b) Анализ возможных рисков и потенциальных негативных последствий.

7. Анализ эффективности:

a) Оценка экономической эффективности проектов, включая расчет показателей возврата инвестиций (ROI), периода окупаемости и дисконтированной стоимости.

b) Сравнение затрат и выгод, чтобы определить общую эффективность проектов.

8. Принятие решения и планирование реализации:

a) Принятие решения о реализации проектов на основе оценки и анализа эффективности.

b) Планирование реализации проектов, включая выделение ресурсов, управление рисками и контроль выполнения.

9. Мониторинг и оценка результатов:

a) Мониторинг и оценка результатов реализации проектов.

b) Измерение достигнутых показателей и сопоставление с ожидаемыми результатами.

c) Корректировка стратегии и планов в случае необходимости.

Макроэкономическая устойчивость [2] относится к способности экономической системы или страны справляться с внутренними и внешними возмущениями, сохраняя стабильность и уровень производства, занятости и цен на стабильном уровне. Она является важным аспектом экономического развития и может быть достигнута через различные факторы и политики. Некоторые ключевые элементы, которые способствуют макроэкономической устойчивости, включают:

1. Фискальная политика: Ответственное управление государственными финансами, включая установление сбалансированного бюджета, контроль

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

государственного долга и эффективное использование государственных доходов и расходов.

2. Монетарная политика: Эффективное управление денежной массой, процентными ставками и контролем инфляции. Центральные банки играют важную роль в осуществлении монетарной политики и поддержании стабильности финансовой системы.

3. Регулирование финансовых рынков: Развитие и применение эффективных нормативных и контрольных механизмов для обеспечения прозрачности, стабильности и честности на финансовых рынках. Контроль рисков и предотвращение чрезмерного уровня задолженности и финансовых пузырей.

4. Стабильность внешней торговли: Поддержание сбалансированных торговых отношений с другими странами, предотвращение чрезмерного дефицита счета текущих операций и обеспечение устойчивости валютного курса.

5. Гибкий рынок труда: Наличие механизмов, способствующих адаптации рынка труда к изменяющимся экономическим условиям, уровню безработицы и включению всех слоев населения в экономический процесс.

6. Инвестиционная среда и предпринимательство: Развитие благоприятной инвестиционной среды, стимулирование предпринимательской активности, инноваций и развития малого и среднего бизнеса.

7. Социальная политика: Обеспечение социальной справедливости, доступности образования и здравоохранения, снижение неравенства и бедности, что способствует устойчивому развитию экономики.

8. Государственные резервы: Создание резервов и стабилизационных фондов для смягчения экономических колебаний и обеспечения финансовой безопасности. Взаимодействие этих факторов и политик в экономическом процессе способствует макроэкономической устойчивости, обеспечивая стабильность и устойчивый рост экономики в долгосрочной перспективе.

Информационная безопасность и экономические системы имеют важное взаимодействие, поскольку безопасность информации и данных является неотъемлемой частью современного бизнеса и экономической деятельности. Вот некоторые основные аспекты этого взаимодействия:

1. Защита конфиденциальности и конкурентоспособности: В экономических системах информация является одним из наиболее ценных активов. Защита конфиденциальности коммерческой информации,

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

интеллектуальной собственности, клиентских данных и других конкурентных сведений является критической для сохранения конкурентоспособности и успеха предприятия.

2. Сохранение целостности данных: Целостность данных в экономической системе важна для обеспечения надежности и точности бизнес-процессов, финансовой отчетности и других операций. Нарушение целостности данных может привести к ошибкам, потере доверия клиентов и финансовым потерям.

3. Обеспечение доступности и непрерывности: Безопасность информации также связана с обеспечением доступности данных и бесперебойной работы экономических систем. Нарушение доступности, например, из-за кибератак или технических сбоев, может привести к простою бизнеса, потере доходов и ухудшению репутации.

4. Управление рисками и снижение потерь: Информационная безопасность помогает экономическим системам управлять рисками, связанными с кибербезопасностью, мошенничеством, нарушениями данных и другими угрозами. Снижение возможных потерь и репутационных рисков способствует устойчивости экономической системы.

5. Регуляторные требования и законодательство: Многие страны имеют законодательные акты и нормативные требования в отношении информационной безопасности, особенно в отношении защиты персональных данных и финансовой отчетности. Соблюдение таких требований является обязательным и может иметь финансовые и юридические последствия для экономических систем.

6. Доверие клиентов и партнёров: Сильная информационная безопасность способствует установлению доверия клиентов, партнеров и инвесторов. Компании, которые могут обеспечить безопасность и защиту данных, часто предпочитаются при выборе партнеров или при принятии решения о сотрудничестве. В целом, информационная безопасность является неотъемлемой частью экономических систем и имеет прямое влияние на их эффективность, конкурентоспособность, надежность и доверие. Безопасность информации должна быть учтена и внедрена на всех уровнях экономических систем, начиная с технических мер безопасности и заканчивая политиками, процедурами и обязательными требованиями, чтобы обеспечить устойчивость и успешное функционирование экономических систем.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

Рис.2 Объекты критической информационной инфраструктуры в экономической системе [3]

Объекты критической информационной инфраструктуры (КИИ) в экономической системе могут варьироваться в зависимости от конкретной страны или сектора экономики. Однако, в общем случае, некоторые типичные объекты КИИ, которые имеют важное значение для экономической системы, включают:

1. Финансовые институты: Банки, биржи ценных бумаг, платежные системы и другие финансовые организации являются критическими объектами КИИ. Надежная и безопасная работа этих систем необходима для обеспечения функционирования финансового сектора и выполнения финансовых операций.

2. Государственные учреждения и административные системы: Государственные органы, включая министерства, налоговые службы, системы государственного управления и другие административные системы, имеют критическую роль в экономической системе. Они обрабатывают и хранят большое количество чувствительной информации, включая персональные данные граждан и бизнесов, а также информацию о внешней торговле и законодательстве.

3. Критическая инфраструктура энергетики: Энергетические системы, включая электроэнергетические сети и энергетические компании, являются важными объектами КИИ. Надежное энергоснабжение необходимо для функционирования промышленности, коммерческих предприятий и повседневной жизни.

4. Телекоммуникационная инфраструктура: Телекоммуникационные сети и провайдеры связи являются неотъемлемой

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

частью экономической системы. Они обеспечивают связь и передачу данных между предприятиями, организациями и индивидуальными пользователями.

5. Транспортные системы: Транспортные сети, включая авиацию, железные дороги, морские порты и дороги, имеют важное значение для экономической активности и перемещения товаров и людей. Безопасность и надежность транспортных систем являются ключевыми аспектами КИИ.

6. Здравоохранение: Системы здравоохранения, включая больницы, лаборатории и медицинские организации, играют критическую роль в обеспечении здоровья населения и функционирования экономики. Защита медицинской информации и обеспечение безопасности медицинских систем являются важными аспектами КИИ.

7. Промышленные системы: Производственные предприятия, заводы и промышленные системы, включая критическую инфраструктуру, такую как ядерные электростанции или химические заводы, могут быть также включены в категорию КИИ. Они имеют важное значение для производства товаров и услуг, а также для обеспечения экономической стабильности и безопасности.

Нарушение работы КИИ может привести к:

I. Перебоям в электроснабжении, транспортном сообщении, связи.
II. Финансовым потерям.
III. Сбоям в работе государственных органов.
IV. Ухудшению качества медицинского обслуживания.
V. Остановке работы промышленных предприятий.
VI. Социальным волнениям.

В связи с этим, обеспечение безопасности КИИ является одной из важнейших задач государства. Для защиты КИИ используются различные меры:

- Законодательное регулирование: принятие законов и подзаконных актов, направленных на защиту КИИ.

- Техническая защита: внедрение систем информационной безопасности, средств защиты информации.

- Организационные меры: разработка и реализация планов защиты КИИ, обучение персонала.

- Международное сотрудничество: обмен опытом по защите КИИ, участие в международных проектах.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

Обеспечение безопасности КИИ – это комплексная задача, которая требует постоянного внимания и усилий. Государство, бизнес и общество должны работать вместе, чтобы защитить КИИ от угроз.

Киберрезилиенция — это концепция, которая относится к способности организации или системы справиться с кибератаками, восстановиться после них и продолжить нормальное функционирование. Экономика, в свою очередь, [3] описывает производство, распределение и потребление товаров и услуг в рамках определенной страны или региона. С учетом растущей численности и сложности кибератак в современном мире, киберрезилиенция становится все более важной для экономики. Кибератаки могут иметь серьезные последствия для бизнеса и государственных организаций, включая финансовые потери, утечку конфиденциальных данных, нарушение производственных процессов и повреждение репутации.

Рис.3 Экономическое состояние Узбекистана после пандемии [4]

В последнее время в Узбекистане введен ряд новых показателей, которые отслеживаются в режиме реального времени и на постоянной основе, давая полное и объективное представление о процессах и тенденциях, происходящих в экономической и социальной сферах. Основные макроэкономические показатели и новые дополнительные индикаторы свидетельствуют о динамичном процессе восстановления экономики.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-4| 2024 Published: |22-04-2024|

Экономические индикаторы — это показатели, отражающие состояние и развитие национальной экономики, а также то, что она находится на той или иной стадии экономического цикла. Типичными примерами являются ВВП, инфляция, золото валютные резервы, ставки рефинансирования, непогашенный государственный долг, платежный баланс, уровень безработицы и ряд финансовых показателей.

Существуют также экономические показатели, рассчитываемые независимыми организациями и институтами. К ним относятся показатели производственной активности, настроения потребителей, деловая уверенность и экономические ожидания. В целом экономические индикаторы отражают изменения в совокупной экономической активности.

После введения карантина в марте 2020 года также будет проводиться мониторинг влияния пандемии на социально-экономическое положение и здоровье населения, для чего будет проведено более 18000 опросов 12 марта 2021года, влияние пандемии на социально-экономическое положение и здоровье населения в период с апреля 2020 года по январь 2021года. Опубликованы результаты опроса о влиянии пандемии на социально-экономическое положение и здоровье населения.

Согласно результатам исследования, в последние месяцы прошлого года председатель сообщил о снижении количества обращений граждан за социальной помощью. Количество новых заявлений на получение пособий по уходу за ребенком для семей с детьми (до двух лет) снизилось: 58%махаллей в августе (2020г.) и 28%в январе 2021г.Количество новых заявлений на получение пособий для малообеспеченных семей с детьми (от двух лети старше)за тот же период снизилось с 51%махаллей до 32.Количество заявлений на другие пособия для малообеспеченных семей(несвязанные с наличием ребенка в семье)снизилось с 56%заявлениймахарав августе (2020) до 21% в январе 2021 года. В августе прошлого года 46% рассматривали возможность обращения за другими социальными пособиями, но к 2021 году этот показатель снизился почти до нуля.

Стоит отметить, что снижение количества обращений граждан за экстренной и социальной помощью является явным показателем того, что экономическое положение населения постепенно улучшается и, как следствие, все меньше людей нуждаются в данном виде помощи. В целом с апреля 2020 года около 5,2 миллиона человек хотя бы раз получали экстренную помощь. В апреле 2020 года менее половины респондентов указали, что кто-то из членов их дом о хозяйства смог продолжить работу

после начала карантина. Хотя многие из первоначальных перерывов в трудовой деятельности были временными, темпы восстановления в 2020 году были медленнее, чем до введения карантина. Недостаточная киберрезилиенция может негативно сказаться на экономике. Большие компании могут столкнуться с существенными финансовыми потерями и потерей доверия со стороны клиентов. Государственные организации могут столкнуться с нарушением работы критической инфраструктуры и потерей конфиденциальных данных, что может привести к нарушению общественного порядка и повреждению экономики в целом.

С другой стороны, инвестиции в кибербезопасность и развитие киберрезилиентности могут способствовать экономическому развитию. Компании и государства, которые активно занимаются защитой от киберугроз и имеют планы восстановления после атак, могут быстрее восстановиться и продолжить свою деятельность, минимизируя негативные последствия. Более безопасная киберсреда способствует росту электронной коммерции, цифровизации и инноваций, что в свою очередь может способствовать экономическому росту и конкурентоспособности. Таким образом, киберрезилиенция и экономика тесно связаны. Развитие кибербезопасности и способность эффективно реагировать на кибератаки становятся все более важными факторами для обеспечения стабильности и роста экономики.

Киберпреступления имеют значительные экономические [5] последствия для отдельных компаний, государств и общества в целом. Вот некоторые из них:

1. Финансовые потери: Киберпреступники могут получить доступ к финансовым системам, банковским счетам, кредитным картам и другим финансовым активам. Это может привести к финансовым потерям для отдельных лиц и компаний. Кроме того, компании могут столкнуться с потерями из-за кражи интеллектуальной собственности, нарушения контрактов или потери доверия со стороны клиентов.

2. Снижение производительности: Кибератаки могут привести к нарушению работы компьютерных систем, сетей и инфраструктуры, что может привести к простоям и снижению производительности. Компании могут терять прибыль из-за временной неработоспособности систем или затрат на восстановление после атаки.

3. Репутационный ущерб: Успешные кибератаки могут привести к серьезному ущербу репутации компании. Потеря доверия клиентов и

инвесторов может привести к снижению продаж, убыткам и сокращению рыночной стоимости компании. Восстановление репутации может потребовать значительных усилий и ресурсов.

4. Затраты на кибербезопасность: Компании вынуждены инвестировать в кибербезопасность для защиты от киберугроз. Это включает в себя затраты на оборудование, программное обеспечение, обучение персонала и поддержку специалистов по кибербезопасности. Эти затраты могут быть значительными и оказывать дополнительное давление на бюджеты компаний.

5. Потеря конкурентных преимуществ: Киберпреступники могут воровать интеллектуальную собственность, бизнес-планы и другую конфиденциальную информацию, что может привести к потере конкурентных преимуществ компании. Конкуренты или злоумышленники могут использовать украденную информацию для своей выгоды.

6. Экономическое замедление: Кибератаки могут иметь системный эффект и негативно повлиять на экономическую стабильность и рост. Например, атаки на критическую инфраструктуру, такую как энергетические сети или финансовые системы, могут вызвать серьезные последствия для экономики страны.

В целом, киберпреступления представляют серьезную угрозу для экономической стабильности и процветания. Улучшение мер безопасности, обучение персонала и международное сотрудничество играют важную роль в предотвращении и борьбе с этой проблемой.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. https://intuit.ru/
2. https://www.smart-soft.ru/
3. https://www.sravni.ru/enciklopediya/info
4. https://www.cer.uz/en/post/publication/uzbekistan-v-indikatorah-vosstanovlenia
5. https://www.tadviser.ru/
6. Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.
7. Anderson, R., & Moore, T. (2014). Economics of Information Security and Privacy. Springer.