

GLOBAL RAQAMLASHTIRISH SHAROITIDA KIBERXAVFSIZLIK MUAMMOLARI VA AXBOROT TIZIMLARINI HIMOYA QILISH STRATEGIYALARI

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ И СТРАТЕГИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Ashurov I.

*Tadqiqotchi, Samarqand davlat universiteti /
Исследователь, Самаркандский
государственный университет
ashurov@gmail.com*

Annotatsiya: Zamonaviy raqamli iqtisodiyot va global raqamlashtirish sharoitida kiberxavfsizlikni ta'minlash muammolari, kiberhujumlarning turlari va axborot tizimlarini himoya qilish mexanizmlari ikki tilda tizimli tahlil qilingan. Maqolada kiberxavf-xatarlarni baholashning matematik modellari ko'rsatilgan.

Аннотация: В условиях современной цифровой экономики и глобальной цифровизации системно на двух языках проанализированы проблемы обеспечения кибербезопасности, виды кибератак и механизмы защиты информационных систем. В статье представлены математические модели оценки киберрисков.

Kalit so'zlar / Ключевые слова: kiberxavfsizlik, kiberhujum, kriptografiya, axborot xavfsizligi, киберпространство, криптографические методы.

1. KIRISH / ВВЕДЕНИЕ

[O'zbekcha] Global raqamlashtirish, bulutli texnologiyalar va narsalar interneti (IoT) tizimlarining shiddatli rivojlanishi davlat organlari, yirik korxonalar va oddiy shaxslarning ma'lumotlar xavfsizligini ta'minlash masalasini eng dolzarb muammolardan biriga aylantirdi. Bugungi kunda kiberxavfsizlik — bu nafaqat kompyuter tizimlarini himoya qilish, balki milliy xavfsizlik va iqtisodiy barqarorlikning asosiy ustunidir. Kiberhujumlar natijasida yetkazilayotgan yillik moliyaviy zarar dunyo bo'ylab milliardlab dollarni tashkil etmoqda.

[Русский] Глобальная цифровизация, бурное развитие облачных технологий и Интернета вещей (IoT) превратили вопрос обеспечения безопасности данных государственных органов, крупных предприятий и частных лиц в одну из самых актуальных проблем. Сегодня кибербезопасность — это не просто защита компьютерных систем, а главная опора национальной

безопасности и экономической стабильности.

2. ADABIYOTLAR TAHLILI / ОБЗОР ЛИТЕРАТУРЫ

[O'zbekcha] Axborot xavfsizligi va kiberfazodagi tahdidlarni modellashtirish sohasida xalqaro miqyosda Shnayyer, Anderson kabi olimlarning fundamental ishlari mavjud. Ularning tadqiqotlarida kriptografik usullar va tarmoq xavfsizligi protokollarining samaradorligi tahlil qilingan. Raqamli iqtisodiyotda kiberxavfsizlik risklarini iqtisodiy baholash modellari Gordon-Loeb modeli doirasida keng o'rganilgan bo'lib, u korxonalarining axborot xavfsizligiga ajratadigan investitsiyalari samaradorligini optimallashtirishga xizmat qiladi. O'zbekistonda ham oxirgi yillarda raqamli infratuzilmani kiberhujumlardan himoya qilishning huquqiy va uslubiy asoslari faol tadqiq etilmoqda.

[Русский] В области информационной безопасности и моделирования угроз в киберпространстве существуют фундаментальные работы таких международных ученых, как Шнайер и Андерсон. В их исследованиях проанализирована эффективность криптографических методов и протоколов сетевой безопасности. Экономическая оценка рисков кибербезопасности в цифровой экономике широко изучена в рамках модели Гордона-Лоэба, которая служит для оптимизации эффективности инвестиций предприятий в информационную безопасность.

[O'zbekcha] Kiberxavfsizlik sohasidagi asosiy muammolardan biri bu hujum usullarining doimiy ravishda murakkablashib borishi va sun'iy intellekt elementlaridan foydalangan holda amalga oshirilishidir. Shu sababli, himoya tizimlari ham adaptiv bo'lishi lozim.

3. RISK-MENEDJMENT VA MATEMATIK MODELLASHTIRISH / РИСК-МЕНЕДЖМЕНТ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

[O'zbekcha] Axborot tizimiga qilingan muvaffaqiyatli kiberhujum ehtimolligini va buning natijasida yuzaga keladigan moliyaviy risk darajasini matematik modellashtirish yordamida baholash mumkin. Risk miqdori (R) quyidagi formula orqali ifodalanadi:

$$R = P(H) \cdot P(V|H) \cdot L$$

Bu yerda, $P(H)$ — tizimga kiberhujum uyushtirilishining umumiy ehtimolligi, $P(V|H)$ — hujum sodir bo'lgan taqdirda tizimdagi zaiflik (vulnerability) tufayli uning muvaffaqiyatli yakunlanish ehtimoli, L (Loss) — kiberhujum natijasida korxona yoki davlat tizimiga yetkaziladigan to'g'ridan-to'g'ri va bilvosita iqtisodiy zarar miqdoridir.

[Русский] Вероятность успешной кибератаки на информационную систему и уровень возникающего в результате финансового риска можно оценить с помощью математического моделирования. Величина риска (R) выражается следующей формулой, где $P(H)$ — общая вероятность совершения кибератаки, $P(V|H)$ — вероятность успешности атаки из-за уязвимости системы,

L — прямой и косвенный экономический ущерб от атаки.

4. STATISTIK MA'LUMOTLAR VA TAHLIL / СТАТИСТИЧЕСКИЕ ДАННЫЕ И АНАЛИЗ

[O'zbekcha] Kiberxavfsizlik hodisalarini monitoring qilish markazlari ma'lumotlariga ko'ra, oxirgi yillarda feyk saytlar yaratish (fishing) va ma'lumotlarni shifrlab, tovon puli talab qilish (ransomware) hujumlari eng yuqori o'sish sur'atlarini ko'rsatmoqda.

2-jadval. Kiberxavfsizlik monitoringi va hodisalar dinamikasi / Таблица 2.

Мониторинг кибербезопасности и динамика инцидентов

HUJUM TURI / ТИП АТАКИ	YILLIK O'SISH KOEFFITSIYENTI / КОЭФ. РОСТА	MUVAFFAQIYAT DARAJASI / УРОВЕНЬ УСПЕХА	HOZIRGI HIMOYA DARAJASI / УРОВЕНЬ ЗАЩИТЫ
Phishing / Фишинг	1,35	22%	O'rtacha / Средний
Ransomware / Вымогатели	1,45	14%	Past / Низкий
DDoS hujumlar / DDoS-атаки	1,12	35%	Yuqori / Высокий
SQL Injection / SQL-инъекции	1,05	8%	O'rtacha / Средний

[Русский] По данным центров мониторинга кибербезопасности, в последние годы наибольшие темпы роста демонстрируют фишинг и атаки вирусов-вымогателей (ransomware). Приведенная таблица показывает динамику инцидентов и текущий уровень защищенности информационных ресурсов.

5. XULOSA VA TAVSIYALAR / ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

[O'zbekcha] Raqamli dunyoda kiberxavfsizlik milliy iqtisodiyot barqarorligining poydevoridir. Axborot tizimlarini himoya qilish mexanizmlarini faqatgina dasturiy darajada emas, balki xodimlarning kiber-savodxonligini oshirish, xalqaro standartlarni (ISO 27001) joriy etish va proaktiv monitoring tizimlarini (SOC) yo'lga qo'yish orqali takomillashtirish lozim. Matematik risk modellaridan foydalanish korxonalarga xavfsizlik byudjetini to'g'ri taqsimlash imkonini beradi.

[Русский] Кибербезопасность в цифровом мире является основой стабильности национальной экономики. Механизмы защиты информационных

систем необходимо совершенствовать не только на программном уровне, но и путем повышения киберграмотности сотрудников, внедрения международных стандартов (ISO 27001). Использование математических моделей рисков позволяет предприятиям правильно распределять бюджет безопасности.

FOYDALANILGAN ADABIYOTLAR / БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni. - Toshkent, 2022.
2. Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5(4), 438-457.
3. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.