[2]. Mavlonov A.B. Vulnerability assessment and phishing analysis. International scientific and practical conference Smart technologies and innovative approaches in research: building a digital future, Ajou University in Tashkent, "Uzbekistan", February 22, 2025.
[3]. Koblitz N. "A Course in Number Theory and Cryptography" 2nd Edition, Springer-Verlag.
[4]. Kuryazov D.M., Sattarov A.B., Axmedov B.B. Blokli simmetrik shifrlash algoritmlari bardoshligina zamonaviy kriptotahlil usullari bilan baholash. Toshkent, "Aloqachi" nashriyoti, 2017.
[5]. Chuck Easttom. Modern Cryptography. Applied Mathematics for Encryption and Information Security. Mc Graw Hill Education, 2016.
[6]. Венбо Мао. Современная криптография. Теория и практика. Москва–Санкт-Петербург–Киев, Лори Вильямс, 2005.
[7]. Juraev G., Mavlonov A., A public key cryptosystem using matrix over the finite ring // Tatra mountains mathematical publications. 2025, t. 91, № 3.
[8]. Christopher Swenson. Modern Cryptanalysis. Techniques for Advanced Code Breaking. 1.1st Edition. January 23, 2022.
[9]. Фаддеев Д.К., Лекции по алгебре. Москва, «Наука», главная редакция, физико-математической литературы, 1984.

Nazarov Zuhriddin Akbar o'g'li ("Cyber university" davlat universiteti "Matematika va tabiiy fanlar" kafedrasi dotsenti; zuhrov13@gmail.com),
Iskandarov Sarvar Baltabayevich (Abu Rayhon Beruniy nomidagi Urganch davlat universiteti "Matematik tahlil" kafedrasi o'qituvchisi; sarvar.i@urdu.uz),
Ismoilova Munisa Orif qizi (Perfect University "Raqamli texnologiyalar" kafedrasi o'qituvchisi; munisaismoilova9718@gmail.com)

AXBOROT TIZIMLARIGA KIBERHUJUMLAR XAVFINI MARKOV ZANJIRLARI ASOSIDA MODELLASHTIRISH

Annotatsiya. *Zamonaviy sharoitda axborot tizimlariga qaratilgan kiberhujumlar sonining ortib borishi ularning xavfini miqdoriy baholash uchun ishonchli matematik vositalarni talab etadi. Mavjud tavsiyalar asosan sifatiy tavsifga tayanadi va tizim holatlarining vaqt bo'yicha dinamikasini yetarlicha aks ettirmaydi. Ushbu maqolada axborot tizimining xavfsizlik holatlari orasidagi o'tishlarni tavsiflovchi diskret vaqtli Markov zanjirlari asosida xavfni baholash modeli taklif etiladi. Tadqiqotda holatlar fazosi va o'tish ehtimolliklari matritsasi shakllantirilib, statsionar taqsimot hamda o'rtacha qaytish vaqti orqali xavf ko'rsatkichlari aniqlanadi. Model shartli sonli misolda sinovdan o'tkazilib, aniqlash ehtimolligining oshishi tizimning uzoq muddatli buzilish ehtimolligini qanday kamaytirishi ko'rsatib berilgan.*

Kalit so'zlar: *Markov zanjirlari, kiberhujum, xavfni baholash, o'tish ehtimolliklari matritsasi, statsionar taqsimot, stoxastik model, axborot xavfsizligi.*

МОДЕЛИРОВАНИЕ РИСКА КИБЕРАТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ НА ОСНОВЕ ЦЕПЕЙ МАРКОВА

Аннотация. *В современных условиях рост числа кибератак на информационные системы требует надёжных математических инструментов для количественной оценки риска. Существующие рекомендации в основном опираются на качественное описание и недостаточно отражают динамику изменения состояний системы во времени. В данной статье предлагается модель оценки риска на основе дискретных цепей Маркова, описывающая переходы между состояниями безопасности информационной системы. В исследовании сформированы пространство состояний и матрица переходных вероятностей, на основе которых определяются показатели риска через стационарное распределение и среднее время возврата. Модель апробирована на условном числовом примере, показывающем, как повышение вероятности обнаружения снижает долгосрочную вероятность компрометации системы.*

Ключевые слова: *цепи Маркова, кибератака, оценка риска, матрица вероятностей переходов, стационарное распределение, стохастическая модель, информационная безопасность.*

MODELING THE RISK OF CYBERATTACKS ON INFORMATION SYSTEMS BASED ON MARKOV CHAINS

Annotation. *In modern conditions, the growing number of cyberattacks on information systems requires reliable mathematical tools for quantitative risk assessment. Existing guidelines are largely descriptive and do not adequately reflect the time dynamics of system state changes. This article proposes a risk-assessment model based on discrete-time Markov chains describing transitions between the security states of an information system. The study formalizes the state space and the transition probability matrix,*

from which risk indicators are derived through the stationary distribution and the mean recurrence time. The model is tested on a conditional numerical example, showing how an increase in detection probability reduces the long-run probability of system compromise.

Keywords: *Markov chains, cyberattack, risk assessment, transition probability matrix, stationary distribution, stochastic model, information security.*

Kirish. So‘nggi yillarda raqamli transformatsiya jarayonlarining jadal rivojlanishi axborot tizimlarining jamiyat va iqtisodiyot hayotidagi o‘rnini tubdan o‘zgartirdi. Davlat boshqaruvi, moliya-bank tizimi, sog‘liqni saqlash, ta‘lim va ishlab chiqarish sohalarida axborot-kommunikatsiya texnologiyalaridan foydalanish ko‘lamining kengayishi bilan bir qatorda, ushbu tizimlarga qaratilgan kiberhujumlar soni va murakkabligi ham sezilarli darajada ortib bormoqda. Bu holatlar esa axborot xavfsizligini ta‘minlash masalasini nafaqat texnik, balki strategik boshqaruv darajasidagi muammoga aylantirmoqda.

Mavjud amaliyotda axborot xavfsizligi xavflarini baholash, asosan, ISO/IEC 27005 va NIST SP 800-30 kabi xalqaro standartlarda tavsiya etilgan sifatiy va ekspert baholash usullariga tayanadi (1) va [2]ga qarang. Bunday yondashuvlar tizimning umumiy xavfsizlik holatini tavsiflashda foydali bo‘lsada, ular tizim holatlarining vaqt o‘tishi bilan qanday o‘zgarishini, ya‘ni, xavfsiz holatdan buzilish holatiga o‘tish dinamikasini yetarlicha miqdoriy tarzda ifodalay olmaydi. Natijada xavfsizlik siyosatini shakllantiruvchi mutaxassislar tizimning uzoq muddatli xavf darajasini prognoz qilishda cheklangan imkoniyatlarga ega bo‘lib qolmoqda.

Ushbu muammoning yechimlaridan biri sifatida ehtimollar nazariyasining stoxastik jarayonlar bo‘limiga mansub Markov zanjirlari apparatidan foydalanish taklif etiladi. Markov zanjirlari tizimning holatdan holatga o‘tish jarayonini ehtimollik nuqtai nazaridan formal tarzda tavsiflash imkonini beradi va nisbatan oz sonli parametrlar, xususan o‘tish ehtimolliklari asosida tizimning uzoq muddatli harakati haqida xulosa chiqarishga xizmat qiladi. Bu xususiyat, ayniqsa, hujumlar to‘g‘risida yetarli statistik ma‘lumotga ega bo‘lmagan tashkilotlar uchun muhim ahamiyat kasb etadi.

Tadqiqotning maqsadi axborot tizimining xavfsizlik holatlari orasidagi o‘tishlarni tavsiflovchi diskret vaqtli Markov zanjiriga asoslangan xavfni baholash modelini ishlab chiqish va uning amaliy qo‘llanilishini shartli sonli misolda asoslashdan iborat. Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi:

– mavzuga oid mavjud ilmiy-metodologik yondashuvlarni tahlil qilish va ularning kuchli hamda zaif tomonlarini aniqlash;

– axborot tizimining xavfsizlik holatlari fazosini va ular orasidagi o‘tish ehtimolliklari matritsasini formal tarzda shakllantirish;

– statsionar taqsimot va o‘rtacha qaytish vaqti tushunchalari orqali xavf ko‘rsatkichlarini aniqlash usulini taklif etish;

– taklif etilgan modelni shartli sonli misolda sinovdan o‘tkazish va natijalarni tahlil qilish.

Tadqiqotning obyekti sifatida axborot xavfsizligi xavflarini boshqarish jarayonlari, tadqiqotning predmeti sifatida esa axborot tizimining xavfsizlik holatlari orasidagi o‘tish dinamikasini tavsiflovchi matematik usullar olingan. Tadqiqotning ilmiy yangiligi shundan iboratki, unda kam statistik ma‘lumotga ega tizimlar uchun ham qo‘llash mumkin bo‘lgan, statsionar taqsimot va o‘rtacha qaytish vaqti tushunchalariga asoslangan sodda hisoblash sxemasi taklif etilgan bo‘lib, u axborot xavfsizligi bo‘yicha amaliy risk-menejment vazifalarini yechishda, shuningdek, ilmiy tadqiqot ishlarida boshlang‘ich uslubiy asos sifatida foydalanilishi mumkin.

Adabiyotlar tahlili. Axborot xavfsizligi xavflarini baholash muammosi xalqaro ilmiy adabiyotda turli yo‘nalishlarda o‘rganilgan. Birinchi yo‘nalishni normativ-metodologik hujjatlar tashkil etadi. Xususan, ISO/IEC 27005:2022 standarti tashkilotlarda axborot xavfsizligi xavflarini boshqarish jarayonini tartibga soluvchi umumiy metodologik asosni belgilaydi [1]. NIST SP 800–30 esa xavfni baholash-ning bosqichma-bosqich amaliy tartibini tavsiflaydi [2]. Ushbu hujjatlar keng qo‘llanilgan, ammo ular asosan past, o‘rta va yuqori shkalalar hamda ekspert baholariga tayanadi. Bu esa, o‘z navbatida, natijalarning subyektivligini oshiradi va tizim holatining vaqt bo‘yicha o‘zgarish dinamikasini hisobga olmaydi.

Ikkinchi yo‘nalishni miqdoriy, jumladan, hujum grafiklariga asoslangan yondashuvlar tashkil etadi. Hoang tomonidan taklif etilgan modelda Markov zanjiri va Common Vulnerability Scoring System ko‘rsatkichlari birlashtirilib, bulutli hisoblash tizimlarida xavfsizlik tahdidlarining ehtimollik taqsimotini hisoblash usuli ishlab chiqilgan [3]. Abraham va Nair tomonidan taklif etilgan modelda esa yutuvchi Markov zanjirlari yordamida kiberxavfsizlikni miqdoriy baholashning stoxastik modeli asoslab berilgan, unda tizimning ishonchliligi va tayyorligi ko‘rsatkichlari hisoblab chiqilgan [4]. Bunday yondashuvlar yuqori

aniqlikka ega, lekin ular odatda batafsil zaiflik va hujum grafigi ma'lumotlarini talab qiladi, bu esa ularni amaliyotda qo'llashni murakkablashtiradi.

Uchinchi yo'nalish sifatida Markov zanjirlariga asoslangan anomaliyalarni aniqlash va hujumlar dinamikasini modellashtirish ishlarini ko'rsatish mumkin. Y.Zhang va Borrorlar tomonidan ishlab chiqilgan modelda kompyuter tizimining normal faoliyat profili Markov zanjiri ko'rinishida shakllantirilib, kuzatilayotgan faoliyatning ushbu profilga mos kelish ehtimolligi asosida anomaliyalar aniqlanadi [5]. Liu, Xing, Wang va Hular tomonidan olib borilgan tadqiqotda esa uzluksiz vaqtli Markov zanjiri va chekli Markov jarayoni yordamida ketma-ket kiberhujumlarning vaqt bo'yicha rivojlanishi modellashtirilgan hamda bank ilovasiga qaratilgan troyan hujumi misolida model sinovdan o'tkazilgan [6]. Bundan tashqari, Patel va Zaveri tomonidan axborot tizimlariga qaratilgan kiberhujumlar uchun risk-baholash modeli taklif qilingan [7]. Ramos va boshqalar esa tarmoq xavfsizligi ko'rsatkichlarini miqdoriy baholashga bag'ishlangan yondashuvlarni tizimli tahlil qilgan [8].

O'tkazilgan tahlil shuni ko'rsatadiki, mavjud Markov zanjiri asosidagi modellarning aksariyati murakkab tizimlar, xususan, bulutli infratuzilma va yirik tarmoqlar uchun mo'ljallangan bo'lib, ular katta hajmdagi tarixiy ma'lumot yoki batafsil hujum grafigini talab qiladi. Shu bilan birga, ehtimollar nazariyasining klassik apparati bo'lgan statsionar taqsimot va o'rtacha qaytish vaqti tushunchalari orqali kam ma'lumotga ega, kichik va o'rta hajmdagi axborot tizimlari uchun sodda va amaliy jihatdan qo'llash oson bo'lgan baholash sxemasi ishlab chiqilishi masalasi yetarlicha o'rganilmagan. Bu esa ushbu tadqiqotning dolzarbligini belgilaydi.

Tadqiqot metodologiyasi. Taklif etilayotgan model diskret vaqtli, chekli holatlar fazosiga ega bo'lgan Markov zanjiri nazariyasiga asoslanadi.

$(\Omega, \mathcal{F}, \mathsf{P})$ ehtimollik fazosida $\{\xi_{n+1}^{(i)};\ n \in \mathbb{N}_0,\ i \in \mathbb{N}\}$ bog'liqsiz, bir xil taqsimlangan va nomanfiy butun qiymatlarni qabul qiluvchi tasodifiy miqdorlar ketma-ketligi bo'lsin, bu yerda $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$ va $\mathbb{N} = \{1, 2, 3, \ldots\}$. Axborot tizimining xavfsizlik holati har bir $t \in \mathbb{N}_0$ vaqt kesimida quyidagi to'rtta holatdan biriga tegishli deb qaraladi:

S_0 — **xavfsiz holat:** tizim normal, aniqlangan zaifliklarsiz ishlamoqda;

S_1 — **zaiflik aniqlangan holat:** tizimda potensial zaif tomon yoki shubhali faollik qayd etilgan, ammo faol hujum kuzatilmagan;

S_2 — **hujum ostidagi holat:** tizimga nisbatan faol hujum amalga oshirilmoqda;

S_3 — **buzilgan holat:** hujum natijasida tizimning konfidensialligi, yaxlitligi yoki mavjudligi buzilgan.

Faraz qilaylik, $\{X(t),\ t \geq 0\}$ jarayonning o'tish ehtimolliklari $k \in \mathbb{N}_0$ uchun

$$P_{ij}(n) := \mathsf{P}(Z(n+k) = j \mid Z(k) = i)$$

bo'lsin. Agar barcha $i, j \in \mathbb{N}_0$ lar uchun

$$\mathsf{P}(Z(n) = j \mid Z(0) = i) = \mathsf{P}(Z(n+k) = j \mid Z(k) = i)$$

bo'lsa, ya'ni, o'tish ehtimolliklari $k \in \mathbb{N}$ ga bog'liqsiz bo'lsa, u holda jarayon vaqtga nisbatan bir jinsli deyiladi. Demak, jarayon bir jinsli aniqlangan bo'lishi uchun uning o'tish ehtimolliklari vaqtga bog'liq bo'lmasligi kerak. Holatlar fazosi $S := \{S_0, S_1, S_2, S_3\}$ chekli bo'lib, $\{X(t),\ t \geq 0\}$ tasodifiy jarayon Markov xossasiga ega, ya'ni, $P_{ij}(1) := \mathsf{P}(X(k+1) = j \mid X(k) = i_k)$ uchun

$$P_{ij} = \mathsf{P}(X(k+1) = j \mid X(k) = i_k, X(k-1) = i_{k-1}, \ldots, X(0) = i_0)$$

tenglik o‘rinli bo‘lsin, bu yerda $P_{ij} := P_{ij}(1)$. Demak, tizimning kelgusi holati faqat joriy holatga bog‘liq bo‘lib, o‘tmishdagi holatlar ta‘sirini hisobga olmaydi. Bu esa modelning asosiy farazi bo‘lib, real tizimlarda qisman cheklovga ega, biroq amaliy hisob-kitoblarni sezilarli darajada osonlashtiradi.

O‘tish ehtimolliklari

$$P_{ij} = \mathsf{P}(X(k+1) = S_j \mid X(k) = S_i),$$

o‘tish ehtimolliklari matritsasi esa $\mathsf{A} = [P_{ij}]$ 4×4 o‘lchamli ko‘rinishda yig‘iladi, bunda har bir qator yig‘indisi birga teng, ya’ni barcha $i \in \mathbb{N}_0$ uchun $\sum_j P_{ij} = 1$.

Matritsaning n – qadamli darajasi Kolmogorov-Chapman tenglamasi orqali topiladi. Agar zanjir irreduktiv va aperiodik bo‘lsa, u holda yagona statsionar taqsimot $\pi := \{\pi_0, \pi_1, \pi_2, \pi_3\}$ mavjud bo‘lib, u

$$\pi = \pi\mathsf{A}, \quad \sum_i \pi_i = 1$$

chiziqli tenglamalar tizimining yechimi sifatida topiladi. Statsionar taqsimotning i – koordinatasi π_i ti-zimning uzoq muddatli ishlash jarayonida S_i holatida bo‘lish ehtimolligini ifodalaydi. Xavf ko‘rsatkichi sifatida, birinchi navbatda, buzilgan holatning statsionar ehtimolligi π_3 qabul qilinadi, u qanchalik katta bo‘lsa, tizim shunchalik yuqori xavf ostida deb hisoblanadi. Ikkinchi ko‘rsatkich sifatida ergodik Markov zanjirlari nazariyasining mashhur natijasidan foydalaniladi: irreduktiv, chekli holatli Markov zanjiri uchun i – holatga o‘rtacha qaytish vaqti $m_{ii} = 1 / \pi_i$ formulasi bilan aniqlanadi. Demak, $m_{33} = 1 / \pi_3$ kattaligi tizimning o‘rtacha nechta qadamda yana buzilish holatiga qaytishini ko‘rsatadi va u ham amaliy xavf ko‘rsatkichi sifatida talqin etiladi. Ushbu m_{33} miqdor qanchalik katta bo‘lsa, tizim ham shunchalik xavfsiz hisoblanadi.

O‘tish ehtimolliklarini baholash uchun ikki manbadan foydalanish mumkin:

–tizimning xavfsizlik jurnallari asosidagi statistik chastotalar, agar bunday ma‘lumot mavjud bo‘lsa;

–statistik ma‘lumot yetarli bo‘lmagan hollarda ekspert baholash usullari, masalan, Delfi usuli yoki analitik ierarxiya jarayoni, bu esa modelning kam ma‘lumotga ega tashkilotlarda ham qo‘llanilishini ta‘minlaydi.

Tahlil va natijalar. Taklif etilgan modelning amaliy qo‘llanilishini ko‘rsatish maqsadida shartli sonli misol ko‘rib chiqiladi. Statistik ma‘lumot yetarli bo‘lmagan holat uchun ekspert baholash asosida quyidagi o‘tish ehtimolliklari matritsasi qabul qilingan deb faraz qilinadi:

$$\mathsf{A} = \begin{array}{c} \begin{matrix} S_0 & S_1 & S_2 & S_3 \end{matrix} \\ \begin{pmatrix} 0.85 & 0.15 & 0 & 0 \\ 0.4 & 0 & 0.5 & 0.1 \\ 0.3 & 0.2 & 0 & 0.5 \\ 0.8 & 0 & 0 & 0.2 \end{pmatrix} \end{array}$$

Matritsaning har bir qatori aniq jismoniy ma‘noga ega, masalan, 2-qatorda S_1 – holatda tizim 0.4 ehtimollik bilan zaiflik bartaraf etilib, xavfsiz holatga qaytadi, 0.5 ehtimollik bilan hujum boshlanadi (S_2 – holatiga o‘tadi) va 0.1 ehtimollik bilan darhol buzilish holati – S_3 ga o‘tadi.

$\pi = \pi\mathsf{A}$ tenglamalar tizimini $\sum_i \pi_i = 1$ shartida yechish natijasida quyidagi statsionar taqsimot olindi:

$$\pi_0 = 0.756,\ \pi_1 = 0.126,\ \pi_2 = 0.063,\ \pi_3 = 0.055.$$

Demak, uzoq muddatli statsionar rejimda tizim vaqtining taxminan 75.6% ni xavfsiz holatda, 12.6% ni zaiflik aniqlangan holatda, 6.3%ni hujum ostida va 5.5%ni buzilgan holatda o‘tkazadi. Bu esa modelning asosiy natijasi bo‘lgan xavf ko‘rsatkichi hisoblanadi. Mos ravishda, buzilgan holatga o‘rtacha qaytish vaqti

$$m_{33} = 1 / \pi_3 \approx 18.1$$

o‘tish qadamiga teng, ya‘ni, model bo‘yicha tizim o‘rtacha har 18 nazorat siklida bir marta buzilish holatiga tushish xavfiga ega.

Modelning amaliy foydaliligini ko‘rsatish uchun sezuvchanlik tahlili o‘tkazildi: zaiflikni aniqlash va bartaraf etish jarayoni takomillashtirilgan deb faraz qilinib (S_1 —holatdan S_0 —holatga o‘tish ehtimolligi 0.4 dan 0.6 gacha oshirilib, S_1 —holatdan S_2 —holatga o‘tish ehtimolligi mos ravishda 0.5 dan 0.3 gacha kamaytirilib), qayta hisoblash amalga oshirildi. Natijada yangi statsionar taqsimot

$$\pi_0 = 0.795,\ \pi_1 = 0.127,\ \pi_2 = 0.038,\ \pi_3 = 0.04$$

qiymatlarini tashkil etdi. Ko‘rinib turibdiki, buzilgan holatning statsionar ehtimolligi π_3 taxminan 0.055 dan 0.04 gacha, ya‘ni, nisbiy hisobda qariyb 28%ga kamaydi. Bu natija zaiflikni erta aniqlash va tezkor bartaraf etish tadbirlarining tizim xavfsizligiga sezilarli ta‘sir ko‘rsatishini miqdoriy jihatdan tasdiqlaydi va taklif etilgan modelning turli xavfsizlik chora-tadbirlarining nisbiy samaradorligini solishtirish vositasi sifatida ishlatilishi mumkinligini ko‘rsatadi.

Xulosa va takliflar. O‘tkazilgan tadqiqot natijasida axborot tizimlarining xavfsizlik holatlari orasidagi o‘tish dinamikasini tavsiflovchi diskret vaqtli Markov zanjiriga asoslangan xavfni baholash modeli ishlab chiqildi. Statsionar taqsimot va o‘rtacha qaytish vaqti tushunchalari asosida ikkita o‘zaro to‘ldiruvchi xavf ko‘rsatkichi: buzilgan holatning uzoq muddatli ehtimolligi va unga o‘rtacha qaytish vaqti taklif etildi. Shartli sonli misolda ko‘rsatilganidek, model nafaqat tizimning joriy xavf darajasini baholash, balki turli profilaktik chora-tadbirlarning nisbiy samaradorligini miqdoriy taqqoslash imkonini ham beradi.

Modelning amaliy ahamiyati shundan iboratki, u statistik ma‘lumot yetarli bo‘lmagan kichik va o‘rta hajmdagi tashkilotlarda ham, ekspert baholariga tayangan holda, qo‘llanilishi mumkin. Bu esa axborot xavfsizligi sohasi bo‘yicha risk-menejment amaliyotini soddalashtirish imkoniyatini yaratadi.

Shu bilan birga, model quyidagi cheklovlarga ega:

–Markov xossasi real tizimlarda har doim ham to‘liq bajarilmasligi mumkin, bu esa natijalarning aniqligiga ta‘sir ko‘rsatadi;

–o‘tish ehtimolliklarini to‘g‘ri baholash modelning ishonchliligini belgilovchi muhim omil hisoblanadi.

Kelgusi tadqiqotlar doirasida modelni yashirin Markov modellari asosida umumlashtirish, shuningdek, mavjud statistik ma‘lumotlar asosida o‘tish ehtimolliklarini dinamik ravishda yangilab boruvchi Bayes yondashuvi bilan integratsiya qilish istiqbolli yo‘nalishlar sifatida belgilandi.

Foydalanilgan adabiyotlar ro‘yxati:

[1]. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. Geneva, International Organization for Standardization, 2022.

[2]. NIST Special Publication 800–30 Revision 1. Guide for Conducting Risk Assessments. Gaithersburg: National Institute of Standards and Technology, 2012.

[3]. Hoang D.B. A Threat Computation Model Using a Markov Chain and Common Vulnerability Scoring System and Its Application to Cloud Security. Journal of Telecommunications and the Digital Economy, vol. 7, № 1, 2019.

[4]. Abraham S., Nair S. Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains. Journal of Communications and Networks, 2014.

[5]. Ye N., Zhang Y., Borror C.M. Robustness of the Markov-Chain Model for Cyber-Attack Detection. IEEE Transactions on Reliability, vol. 53, № 1, p. 116–123, 2004.

[6]. Liu C., Xing L., Wang C., Hu Q. Probabilistic modeling and analysis of sequential cyber-attacks. Engineering Reports, vol. 1, Issue 5, 2019.

[7]. Patel S., Zaveri J. A risk-assessment model for cyber attacks on information systems. Journal of Computers, vol. 5, № 3, p. 352–359, 2010.

[8]. Ramos A., Lazar M., Holanda F.R., Rodrigues J. Model-Based Quantitative Network Security Metrics: A Survey. IEEE Communications Surveys & Tutorials, vol. 19, № 4, pp. 2704-2734, 2017.

Gulyamov Gafur (Namangan davlat Texnika universiteti, fizika-matematika fanlari doktori, professor; e-mail: gulyamov1949@mail.ru),
Majidova Gulnoza Nurmuxamedovna (Namangan davlat Texnika universiteti, fizika-matematika fanlari nomzodi, dotsent; e-mail: m.gulnoza.1985@gmail.com),
Muxitdinova Feruza Rustam qizi (Namangan davlat Texnika universiteti, fizika-matematika fanlari nomzodi; e-mail: feruzafizik1991@gmail.com),
Sharipova Mashxura Shamshidinovna (Namangan davlat Texnika universiteti, "Fizika" kafedrasi doktoranti, e-mail: sharipova1202qw@gmail.com)

GETEROSTRUKTURA ASOSIDAGI FOTOTRANSIZTORLARNING XARAKTERISTIKALARIGA YORUG'LIKNING TA'SIRI

Annotatsiya. *Ushbu ishda n-p-n o'tishli fototranzistorlarning volt-amper xarakteristikasining turli yorug'lik ta'sirida paydo bo'ladigan fototok hisobiga o'zgarishlari ko'rib chiqilgan. Yorug'lik ta'sirida generatsiyalangan fototok taranzistorni bazasini ochib, tok aktiv rejimda ishlashini ta'minlaydi. Yorug'lik intensivligi ortganda esa bu tok ham ortib, aktiv soha tokining ortishiga olib kelishi ko'rsatilgan. Nazariy ifodalar ishlab chiqilgan va u asosida olingan volt-amper xarakteristikalarining o'zgarishlaridagi fizik asoslari keltirilgan.*

Kalit so'zlar: *n-p-n o'tish, geteroo'tish, fototranzistor, volt-amper xarakteristikasi, emitter, kollektor, baza.*

Гулямов Гафур (Наманганский государственный технический университет, доктор физико-математических наук, профессор; e-mail: gulyamov1949@mail.ru),
Мажидова Гульноза Нурмухамедовна (Наманганский государственный технический университет, кандидат физико-математических наук, доцент; e-mail: m.gulnoza.1985@gmail.com),
Мухитдинова Феруза Рустам кизи (Наманганский государственный технический университет, кандидат физико-математических наук; e-mail: feruzafizik1991@gmail.com),
Шарипова Машхура Шамшидиновна (Наманганский государственный технический университет, докторант, кафедра физики; e-mail: sharipova1202qw@gmail.com)

ВЛИЯНИЕ СВЕТА НА ХАРАКТЕРИСТИКИ ФОТОТРАНЗИСТОРОВ НА ОСНОВЕ ГЕТЕРОСТРУКТУРЫ

Аннотация. *В данной работе рассмотрены изменения вольт-амперных характеристик n-p-n-переходных фототранзисторов вследствие фототока, возникающего под воздействием различных источников света. Фототок, генерируемый под воздействием света, открывает базу транзистора, обеспечивая его работу в активном режиме. Показано, что при увеличении интенсивности света этот ток также увеличивается, что приводит к увеличению тока активного поля. Разработаны теоретические выражения и представлены физические основы изменений вольт-амперных характеристик, полученных на их основе.*

Ключевые слова: *n-p-n переход, гетеропереход, фототранзистор, вольт-амперная характеристика, эмиттер, коллектор, база.*

Gafur Gulyamov (Namangan State Technical University, Doctor of Physical and Mathematical Sciences, Professor; email: gulyamov1949@mail.ru),
Majidova Gulnoza Nurmukhamedovna (Namangan State Technical University, Candidate of Physical and Mathematical Sciences, Associate Professor; email: m.gulnoza.1985@gmail.com),
Mukhitdinova Feruza Rustam kizi (Namangan State Technical University, Candidate of Physical and Mathematical Sciences; email: feruzafizik1991@gmail.com),
Sharipova Mashkhura Shamshidinovna (Namangan State Technical University, Doctoral Candidate, Department of Physics, email: sharipova1202qw@gmail.com)

INFLUENCE OF LIGHT ON THE CHARACTERISTICS OF PHOTOTRANSISTORS BASED ON A HETEROSTRUCTURE

Annotation. *This paper examines changes in the current-voltage characteristics of n-p-n junction phototransistors due to photocurrent generated by various light sources. The photocurrent generated by light opens the transistor's base, enabling its operation in active mode. It is shown that with increasing light intensity, this current also increases, leading to an increase in the active field current. Theoretical*