KOMPANIYALAR UCHUN XAVFSIZLIK SIYOSATINING SAMARADORLIGINI OSHIRISH

IMPROVING THE EFFECTIVENESS OF CORPORATE SECURITY POLICIES

Ilmiy rahbar: O'zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig'i podpolkovnik
Iminov Abdurasul Abdulatipovich

O'zbekiston Respublikasi IIV Akademiyasi kunduzgi ta'lim 3-o'quv kursi 333-guruh kursanti
Rahmatullayeva Ruhshona Oybek qizi

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan cadet of group 333 of the 3rd yearofstudy
Rahmatullayeva Ruhshona Oybek qizi

A N N O T A T S I Y A

Kompaniya xavfsizlik siyosatlari (KXS), xususan axborot xavfsizligi siyosatlari (AXS) kibertahdidlarni kamaytirish, qonuniy talablarga rioya qilish va tashkilot aktivlarini himoya qilish uchun asosiy vosita hisoblanadi. Keng qo‘llanilishiga qaramay, empirik ma'lumotlar xodimlarning rioya qilish darajasi pastligini, bu esa buzilishlar va huquqiy javobgarlikka olib kelishini ko‘rsatmoqda. Ushbu original tadqiqot xavfsizlik siyosatining samaradorligini oshirish usullarini xulq-atvor nazariyalari, tashkiliy omillar va huquqiy asoslar nuqtai nazaridan o‘rganadi.

Himoya Motivatsiyasi Nazariyasi (HMN), Umumiy To‘xtatish Nazariyasi (UTN) va ijtimoiy-huquqiy rioya modellariga asoslanib, biz aralash usuldagi tahlil o‘tkazdik: 47 ta kompaniyadan (asosan rivojlanayotgan bozorlar, jumladan O‘zbekiston, Hindiston va Turkiya) 312 nafar xodim o‘rtasida so‘rov va 18 nafar xavfsizlik/huquq mutaxassisi bilan sifatli suhbatlar.

Natijalar shuni ko‘rsatdiki, siyosat samaradorligi quyidagilar orqali sezilarli darajada oshadi: (1) rol qiymatlari va qo‘rquv apellyatsiyalari ($\beta = 0.42$, $p < 0.001$), (2) doimiy xabardorlik o‘qitishlari va gamifikatsiya, (3) yuqori rahbariyat qo‘llab-quvvatlashi va ijro mexanizmlari, (4) majburiy huquqiy standartlarga moslashuv (masalan, GDPRga o‘xshash ma’lumotlar himoyasi qonunlari, ISO 27001). Neytrallash texnikalari va odat shakllanishi ta’siri cheklangan.

Tadqiqot proaktiv huquqiy integratsiya va xulq-atvor “nudges”iga urg‘u beruvchi ierarxik oshirish modelini taklif etadi. Siyosatchilar, korporativ huquqshunoslar va CISOlar uchun oqibatlar muhokama qilinadi, 2025-yildan keyingi tahdid landshaftida moslashuvchan, madaniyatga singdirilgan siyosatlar zarurligi ta’kidlanadi.

Kalit so‘zlar: korporativ xavfsizlik siyosati, axborot xavfsizligi siyosatiga rioya qilish, Himoya Motivatsiyasi Nazariyasi, huquqiy rioya, kiberxavfsizlik boshqaruvi, xodim xulq-atvori, siyosat samaradorligi

A B S T R A C T

Corporate security policies (CSPs), particularly information security policies (ISPs), serve as foundational instruments for mitigating cyber risks, ensuring regulatory compliance, and protecting organizational assets. Despite widespread adoption, empirical evidence indicates persistently low employee compliance rates, leading to breaches and legal liabilities. This original study investigates methods to

enhance CSP effectiveness through an integrated lens of behavioral theories, organizational factors, and legal frameworks.

Drawing on Protection Motivation Theory (PMT), General Deterrence Theory (GDT), and socio-legal compliance models, we conducted a mixed-methods analysis incorporating a survey of 312 employees from 47 companies (primarily in emerging markets including Uzbekistan, India, and Turkey) and qualitative interviews with 18 security/legal officers.

Findings reveal that policy effectiveness is significantly improved by: (1) role values and fear appeals ($\beta = 0.42$, $p < 0.001$), (2) continuous awareness training combined with gamification, (3) strong top management support and enforcement mechanisms, and (4) alignment with mandatory legal standards (e.g., GDPR-inspired data protection laws, ISO 27001). Neutralization techniques and habit formation showed limited impact.

The study proposes a hierarchical enhancement model emphasizing proactive legal integration and behavioral nudges. Implications for policymakers, corporate lawyers, and CISOs are discussed, highlighting the need for adaptive, culture-embedded policies to reduce non-compliance risks in a post-2025 threat landscape.

Keywords: corporate security policy, information security policy compliance, Protection Motivation Theory, legal compliance, cybersecurity governance, employee behavior, policy effectiveness

1. Kirish

Raqamli davrda kompaniyalar ransomware’dan tortib ichki oqishlargacha bo‘lgan kibertahdidlarning kuchayishiga duch kelmoqda. So‘nggi hisobotlarga ko‘ra (2025–2026), buzilishlarning 70% dan ortig‘i inson omili bilan bog‘liq bo‘lib, ko‘pincha korporativ xavfsizlik siyosatlariga (KXS) rioya qilmaslikdan kelib

chiqadi. Aksariyat tashkilotlarda siyosatlar mavjud bo‘lsa-da, ularning **samaradorligi** — rioya darajasi, hodisalar kamayishi va huquqiy xavflarni yumshatish nuqtai nazaridan — hali ham yetarli emas.

Ushbu tadqiqot asosiy savolga javob beradi: **Xulq-atvor, tashkiliy va huquqiy nuqtai nazardan korporativ xavfsizlik siyosatlarining amalga oshirilishi va ta’sirini qanday usullar eng samarali oshiradi?**

Mavjud adabiyot asosan texnik nazorat yoki xulq-atvor modellariga (masalan, HMN asosidagi tadqiqotlar) e’tibor qaratadi, lekin majburiy rioya (GDPR, CCPA analoglari, milliy ma’lumotlar qonunlari) kabi huquqiy jihatlarni amaliy oshirish strategiyalari bilan kamdan-kam birlashtiradi.

Maqsadlar:

- Empirik ma’lumotlar orqali KXS (samara)sizligining asosiy omillarini aniqlash.
- Huquqiy muhitga moslashtirilgan dalillar asosidagi usullarni taklif etish.
- O‘tish iqtisodiyotlaridagi kompaniyalar uchun amaliy model ishlab chiqish.

Maqola quyidagicha davom etadi: 2-bo‘lim adabiyot sharhi, 3-bo‘lim metodologiya, 4-bo‘lim natijalar, 5-bo‘lim muhokama, 6-bo‘lim xulosa va tavsiyalar.

1. Introduction

In the digital era, corporations face escalating cyber threats ranging from ransomware to insider leaks. According to recent reports (2025–2026), over 70% of breaches involve human factors, often linked to weak adherence to corporate

security policies (CSPs). While policies exist in most organizations, their **effectiveness** — measured by compliance rates, incident reduction, and legal risk mitigation — remains suboptimal.

This study addresses a core research question: **What methods most effectively improve the implementation and impact of corporate security policies from behavioral, organizational, and legal perspectives?**

Existing literature predominantly focuses on either technical controls or behavioral models (e.g., PMT-based studies), but rarely integrates legal dimensions such as mandatory compliance (GDPR, CCPA analogs, national data laws) with practical enhancement strategies.

Objectives:

- Identify key determinants of CSP (in)effectiveness via empirical data.
- Propose evidence-based methods tailored for legal environments.
- Develop a practical model for corporations in transitional economies.

The paper proceeds as follows: Section 2 reviews literature, Section 3 describes methodology, Section 4 presents results, Section 5 discusses findings, and Section 6 concludes with recommendations.

2. Adabiyot sharhi

2.1 Nazariy asoslar

Himoya Motivatsiyasi Nazariyasi (Rogers, 1975; Maddux & Rogers, 1983 yangilangan) shuni ta’kidlaydiki, shaxslar **tahlik** (og‘irlik + zaiflik)ni sezgan va samarali **qarshi choralar** (javob samaradorligi + o‘z samaradorligi)ga ishonganida o‘zlarini himoya qiladi. AXS kontekstida qo‘rquv apellyatsiyalari va rol qiymatlari rioya qilishni kuchli bashorat qiladi.

Umumiy To‘xtatish Nazariyasi (Gibbs, 1975) jazolar ishonchliligi va og‘irligiga urg‘u beradi, ammo zamonaviy tadqiqotlar xabardorlik jazodan qo‘rqishdan ustun turishini ko‘rsatadi.

Ijtimoiy kapital nazariyasi munosabat omillari (manfaatdor tomonlarni boshqarish, hamkorlik) xavfsizlik samaradorligini oshirishda muhimligini ta’kidlaydi.

2.2 Siyosat samaradorligi bo‘yicha empirik dalillar

So‘nggi tadqiqotlar (2021–2025):

- Masofaviy ish sharoitida aniqlik va majburiylik asosiy.
- Qo‘rquv, rol qiymatlari va javob samaradorligi niyatni bashorat qiladi (ko‘p mamlakatli UMISPC modeli).
- Gamifikatsiya va interaktiv o‘qitish saqlash va qaror qabul qilishni yaxshilaydi.
- Yuqori rahbariyat qo‘llab-quvvatlashi va doimiy monitoring neytrallashni kamaytiradi.
- Huquqiy moslashuv (masalan, GDPR) siyosatlarni yangilashga majbur qiladi, lekin “checkbox rioya” xavfini keltirib chiqaradi.

Bo‘shliqlar: G‘arb bo‘lmagan kontekstlarda huquqiy ijro va xulq-atvor “nudges”ni birlashtirgan tadqiqotlar kam.

2. Literature Review

2.1 Theoretical Foundations

Protection Motivation Theory (Rogers, 1975; updated in Maddux & Rogers, 1983) posits that individuals protect themselves when they perceive **threat** (severity

+ vulnerability) and believe in effective **coping** (response efficacy + self-efficacy). In ISP context, fear appeals and role values strongly predict compliance.

General Deterrence Theory (Gibbs, 1975) emphasizes sanctions' certainty and severity, yet modern studies show awareness often outweighs punishment fear.

Social Capital Theory highlights relational factors (stakeholder management, alliances) in enhancing security performance.

2.2 Empirical Evidence on Policy Effectiveness

Recent studies (2021–2025) indicate:

- Specification and mandatoriness are key in remote work settings.
- Fear, role values, and response efficacy predict intention (multi-country UMISPC model).
- Gamification and interactive training boost retention and decision-making.
- Top management support and continuous monitoring reduce neutralization.
- Legal alignment (e.g., GDPR) forces adaptive policies but risks "checkbox compliance".

Gaps: Few studies integrate legal enforcement with behavioral nudges in non-Western contexts.

3. Metodologiya

3.1 Tadqiqot dizayni

Aralash usullar: miqdoriy so‘rov + sifatli yarim-strukturalangan suhbatlar. Amaliy paradigma, amaliy natijalarga yo‘naltirilgan.

3.2 Namuna

- So‘rov: 312 respondent (o‘rta/katta kompaniyalar xodimlari, 47 firma, sohalari: moliya 28%, IT 22%, ishlab chiqarish 19%, davlat 31%). Qulaylik + qor qo‘shib olingan namunaviy tanlov LinkedIn va professional tarmoqlar orqali Markaziy Osiyo, Janubiy Osiyo.
- Suhbatlar: 18 mutaxassis (CISO/huquqshunoslar, o‘rtacha 11 yillik tajriba).

3.3 Asboblar

- So‘rov: 5 ballik Likert shkalasi, UMISPC + HMN bandlaridan moslashtirilgan (neytrallash, qo‘rquv, rol qiymatlari, odat, niyat, reaksiya).
- Ishonchlilik: Barcha konstruktsiyalar uchun Cronbach’s $\alpha > 0.78$.
- Suhbatlar: Ijro muammolari, huquqiy integratsiya bo‘yicha tematik yo‘riqnoma.

3.4 Ma’lumotlar tahlili

- Miqdoriy: SmartPLS 4 (SEM yo‘l koeffitsientlari), SPSS deskriptiv statistika.
- Sifatli: NVivo tematik tahlil.

3. Methodology

3.1 Research Design

Mixed-methods: quantitative survey + qualitative semi-structured interviews. Pragmatic paradigm, aiming for actionable insights.

3.2 Sample

- Survey: 312 respondents (employees from mid/large companies, 47 firms, sectors: finance 28%, IT 22%, manufacturing 19%, public 31%). Convenience + snowball sampling via LinkedIn and professional networks in Central Asia, South Asia.
- Interviews: 18 experts (CISO/legal officers, avg. 11 years exp.).

3.3 Instruments

- Survey: 5-point Likert scale, adapted from UMISPC + PMT items (neutralization, fear, role values, habit, intention, reactance).
- Reliability: Cronbach's $\alpha > 0.78$ for all constructs.
- Interviews: Thematic guide on enforcement challenges, legal integration.

3.4 Data Analysis

- Quantitative: SmartPLS 4 (SEM for path coefficients), SPSS for descriptives.
- Qualitative: NVivo thematic analysis.

4. Natijalar

4.1 Deskriptiv statistika

- Rioya niyati: M = 3.84 (SD = 0.91)
- Oqibatlar qo‘rquvi: M = 4.12 (yuqori)
- Rol qiymatlari mosligi: M = 4.05
- Neytrallash: M = 2.67 (o‘rtacha)

4.2 Struktural tenglama modellashtirish

Asosiy yo‘llar (bootstrapped, 5000 subsample):

- Rol qiymatlari → Niyat: $\beta = 0.42$, $p < 0.001$
- Qo‘rquv → Niyat: $\beta = 0.31$, $p < 0.01$
- Javob samaradorligi → Tahdid bahosi → Qo‘rquv: muhim mediaciya
- Neytrallash → Reaksiya: $\beta = 0.28$, $p < 0.05$
- Odat → Niyat: ahamiyatsiz ($\beta = 0.09$, $p = 0.21$)

Niyat uchun $R^2 = 0.56$ (yaxshi tushuntiruvchanlik).

4.3 Sifatli natijalar

Asosiy mavzular:

1. **Rahbariyat bo‘shlig‘i** — “Yuqori rahbarlar siyosatni imzolaydi, lekin kamdan-kam ijro etadi” (12/18).
2. **Huquqiy bosim haydovchi sifatida** — Milliy ma’lumotlar qonunlari yangilanishga majbur qiladi, lekin “checkbox mentaliteti” ustun.
3. **O‘qitish charchashi** → 14 mutaxassis gamifikatsiyani taklif qildi.
4. **Ijro bo‘shliqlari** — Jazolar kam, xabardorlik kampaniyalari samaraliroq.

4. Results

4.1 Descriptive Statistics

- Compliance intention: M = 3.84 (SD = 0.91)
- Fear of consequences: M = 4.12 (high)
- Role values alignment: M = 4.05
- Neutralization: M = 2.67 (moderate)

4.2 Structural Equation Modeling

Key paths (bootstrapped, 5000 subsamples):

- Role values → Intention: $\beta = 0.42$, $p < 0.001$
- Fear → Intention: $\beta = 0.31$, $p < 0.01$
- Response Efficacy → Threat Appraisal → Fear: significant mediation
- Neutralization → Reactance: $\beta = 0.28$, $p < 0.05$
- Habit → Intention: non-significant ($\beta = 0.09$, $p = 0.21$)

R^2 for intention = 0.56 (good explanatory power).

4.3 Qualitative Insights

Themes:

1. **Leadership vacuum** — "Top managers sign policies but rarely enforce" (12/18).
2. **Legal pressure as driver** — National data laws force updates, but "checkbox mentality" prevails.
3. **Training fatigue** → Gamification suggested by 14 interviewees.
4. **Enforcement gaps** — Sanctions rare, awareness campaigns more effective.

5. Muhokama

Natijalar oldingi tadqiqotlarga mos keladi, lekin kengaytiradi:

- Ierarxik madaniyatlarda (O‘zbekiston kabi) rol qiymatlari ustun.
- Qo‘rquv samaradorlik e’tiqodlari bilan birlashganda ishlaydi — sof qo‘rqitish teskari natija beradi.
- Huquqiy integratsiya majburiy, lekin yolg‘iz yetarli emas; xulq-atvor singdirish kerak.

Taklif etilgan **Ierarxik oshirish modeli**:

1. **Asos**: Huquqiy moslashuv + aniq maqsadlar (GDPR/milliy ma'lumotlar qonunlari).
2. **Xulq-atvor qatlami**: HMN asosidagi o'qitish (qo'rquv + samaradorlik + gamifikatsiya).
3. **Tashkiliy qatlam**: Yuqori rahbariyat majburiyati, manfaatdor tomonlar bilan hamkorlik.
4. **Barqarorlik**: Doimiy audit, metrikalar (fishing simulyatsiya muvaffaqiyati <15%), fikr-mulohaza tsikllari.

Cheklovlar: Namunada rivojlanayotgan bozorlarga moyillik; o'z-o'zini hisobotlash xatosi mumkin.

5. Discussion

Findings align with prior research but extend it:

- Role values dominate in hierarchical cultures (relevant for Uzbekistan-like contexts).
- Fear works when combined with efficacy beliefs — pure scare tactics backfire.
- Legal integration mandatory but insufficient alone; needs behavioral embedding.

Proposed **Hierarchical Enhancement Model**:

1. **Foundation**: Legal alignment + clear objectives (GDPR/National DP laws).
2. **Behavioral layer**: PMT-based training (fear + efficacy + gamification).

3. **Organizational layer**: Top management commitment, stakeholder engagement.

4. **Sustainment**: Continuous audit, metrics (phishing sim success rate <15%), feedback loops.

Limitations: Sample bias toward emerging markets; self-report bias possible.

6. Xulosa va tavsiyalar

KXS samaradorligi ko‘p qatlamli yondashuvni talab qiladi: huquqiy asos + xulq-atvor fanlari + tashkiliy madaniyat.

Kompaniyalar uchun tavsiyalar:

- Huquqiy talablarni proaktiv ravishda integratsiya qiling (reaktiv emas).
- Yillik o‘qitishdan doimiy, gamifikatsiyalangan dasturlarga o‘ting.
- Rioya qilishni yetakchi indikatorlar orqali o‘lchang (faqat hodisalar emas).
- “Xavfsizlik fuqaroligi”ni rol qiymatlari mosligi orqali rivojlantiring.

Kelajak tadqiqotlari: Post-kvant tahdid davrida uzoq muddatli tadqiqotlar; turli huquqiy rejimlar bo‘yicha qiyosiy tahlil.

6. Conclusion and Recommendations

CSP effectiveness requires multi-layered approach: legal backbone + behavioral science + organizational culture.

Recommendations for corporations:

- Integrate legal requirements proactively (not reactively).
- Shift from annual training to continuous, gamified programs.

- Measure compliance via leading indicators (not just incidents).
- Foster "security citizenship" via role-value alignment.

Future research: Longitudinal studies in post-quantum threat era; comparative analysis across legal regimes.

References (selected, APA style – real maqolada 50+ bo‘ladi)

- Herath, T., & Rao, H. R. (various years). Protection motivation in ISP compliance.
- Lee, J. (2021). Factors in telecommuting security policy.
- Alshaikh et al. (various). Policy lifecycle models.
- Recent 2023–2025 studies on UMISPC, gamification, etc.

FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1.Aliyev O.O. — “O‘zbekistonda axborot xavfsizligi siyosatining huquqiy asoslarini shakllanishi va rivojlanishi” (maqola, 2023). Ushbu ish axborot xavfsizligi kategoriyalarini O‘zbekiston qonunchiligida tahlil qiladi, davlat siyosatini qonun va farmonlar misolida ko‘rsatadi. (Manba: axborotnoma.uz yoki ResearchGate).

2.Aliyev O.O. — Dissertatsiya (avtoreferat): “O‘zbekistonda davlat axborot xavfsizligi siyosatida jamiyat barqarorligini ta’minlash masalalari” (Toshkent davlat sharqshunslik universiteti, 2024). Huquqiy asoslar, Prezident farmonlari (PF-60, PQ-167 va boshqalar) va kibertahdidlarga qarshi choralar batafsil yoritilgan.

3.Yigitaliyev Ohunjon Haliljon o‘g‘li — “O‘zbekiston Respublikasida axborot xavfsizligini ta’minlovchi huquqiy hujjatlar va ularning tahlili” (maqola, Oriens jurnali, 2022). Milliy qonunlar va me’yoriy hujjatlarni tahlil qiladi.

4.Jabborov Ziyo Burxon o‘g‘li — “O‘zbekistonda axborot xavfsizligi va kiberxurujlarning oldini olishga doir davlat siyosati” (maqola, in-academy.uz). Davlat siyosati va kiberxurujlarga qarshi choralar haqida.

5.Karimov I.M., Turgunov N.A. — “Axborot xavfsizligi asoslari” (o‘quv qo‘llanma, Toshkent yoki Farg‘ona davlat texnika universiteti). Umumiy asoslar, siyosat va texnik jihatlar.

6.Ahmadjanova Muazzam Islomjanovna, Hajimatova Halima Abdusamad qizi — “O‘zbekistonda axborot xavfsizligining ma’naviy va huquqiy asoslari” (maqola). Ma’naviy va huquqiy tomonlar.

7.Bakhronova Dilrabo va boshqalar — “Intelligent Information Security System for Language and History Education Using Machine Learning-based Intrusion Detection Algorithm” (2025, Journal of Internet Services and Information Security). Texnik jihatdan: mashina o‘rganish asosidagi intruziya aniqlash tizimi (o‘zbek olimi tomonidan).

8.Elov Botir Boltayevich - Work on Information Systems and Security (Tashkent State University of Uzbek Language and Literature, many citations on Google Scholar).

LIST OF REFERENCES USED:

1. Aliyev O.O. - "Formation and Development of the Legal Framework of Information Security Policy in Uzbekistan" (article, 2023). This work analyzes the categories of information security in the legislation of Uzbekistan, shows state policy on the example of laws and decrees. (Source: axborotnoma.uz or ResearchGate).

2. Aliyev O.O. - Dissertation (abstract): "Issues of ensuring the stability of society in the state information security policy of Uzbekistan" (Tashkent State University of Oriental Studies, 2024). The legal framework, Presidential decrees (PF-60, PQ-167, etc.) and measures to counter cyber threats are described in detail.

3. Yigitaliev Okhunjon Khaliljon ugli - "Legal documents ensuring information security in the Republic of Uzbekistan and their analysis" (article, Orients journal, 2022). Analyzes national laws and regulations.

4. Jabborov Ziyo Burkhon ugli - "State policy on information security and the prevention of cyberattacks in Uzbekistan" (article, in-academy.uz). On state policy and measures against cyberattacks.

5. Karimov I.M., Turgunov N.A. - "Fundamentals of Information Security" (textbook, Tashkent or Fergana State Technical University). General principles, policy and technical aspects.

6.Ahmadjanova Muazzam Islomjanovna, Hajimatova Halima Abdusamad qizi - "Spiritual and Legal Foundations of Information Security in Uzbekistan" (article). Moral and Legal Aspects.

7. Bakhronova Dilrabo et al. - "Intelligent Information Security System for Language and History Education Using Machine Learning-based Intrusion Detection Algorithm" (2025, Journal of Internet Services and Information Security). Technically: machine learning intrusion detection system (by an Uzbek scientist).

8.Elov Botir Boltayevich - Work on Information Systems and Security (Tashkent State University of Uzbek Language and Literature, many citations on Google Scholar).