

# ЎЗБЕКИСТОНДА АХБОРОТ ХАВФСИЗЛИГИНИ РИВОЖЛАНТИРИШ ЖАРАЁНИ ВА УНИНГ ИСТИҚБОЛЛАРИ

Алиев Олимбек Ойбекович  
АДУ, Фалсафа кафедраси тадқиқотчиси

## Аннотация

Мақолада ахборот хавфсизлигини ривожлантириш бўйича Ўзбекистонда олиб борилаётган давлат сиёсати ва унинг ҳуқуқий асослари ҳақида фикр юрилган. Шунингдек, ахборот хавфсизлигини ривожлантириш жараёнларида амалга оширилаётган ишлар таҳлил қилиниб, истиқболдаги вазифалар белгиланган.

**Калит сўзлар:** ахборот хавфсизлиги, давлат сиёсати, ҳуқуқий асос, стратегия, кибермайдон, киберхужум, кибертерроризм, киберхавфсизлик, рақамли идентификациялаш, кардинал рақамли трансформация.

## Абстрактный

В статье рассматривается государственная политика развития информационной безопасности в Узбекистане и ее правовая основа. Также была проанализирована работа, проводимая в процессе развития информационной безопасности, и определены задачи на будущее.

**Ключевые слова:** информационная безопасность, государственная политика, правовая база, стратегия, киберпространство, кибератака, кибертерроризм, кибербезопасность, цифровая идентификация, кардинальная цифровая трансформация.

## Abstract

The article discusses the state policy for the development of information security in Uzbekistan and its legal basis. The work carried out in the process of developing information security was also analyzed, and tasks for the future were identified.

**Key words:** information security, public policy, legal framework, strategy, cyberspace, cyber attack, cyber terrorism, cyber security, digital identity, cardinal digital transformation.

Ўзбекистон Республикаси Президентининг 2020 йил 5 октябрдаги ПФ6079-сон фармони билан “Рақамли Ўзбекистон – 2030” стратегияси қабул қилиниб, уни самарали амалга ошириш чора-тадбирлари белгиланиши натижасида бир томондан АКТ такомиллашиб ва кенгайиб борган бўлса, иккинчи томондан, ахборот хавфсизлиги моддий техникавий базасини ривожлантириш жараёнлари ҳам ривожлана бошлади.

Мамлакатда ахборот-коммуникация технологиялари такомиллашиб, ривожланиб ва кенгайиб бориши билан уларга қарши ички ва ташқи киберхужумлар ҳам кучайиб ва кўпайиб борди. Бу, албатта, жамият барқарорлигини бузишга олиб келиши мумкин эди. Жумладан, 2021 йил 6 январда Сурхондарё вилояти, Ангор, Музработ, Шеробод, Қизирик, Бойсун,

Жаркўрғон, Қумқўрғон, Олтинсой, Денов ва Узун туманлари ҳокимликлари расмий сайтлари ахборот хавфсизлигини бузиш учун ҳужумларга учради [1].

2022 йилда ҳар куни ўртача 67 та дастур-юлғичларнинг янги ҳужумлари рўй бериб турди. Техникавий ёрдам билан боғлиқ бўлган товламачилик ходисалари (фуқароларга “хорижий счетлардан пул ўтказиш”ни таклиф қилган қаллоблар) ҳам кўпайди. Бундан кўрилган зиёнлар 347 млн. долларни ташкил этиб, бу кўрсаткич 2020 йилга нисбатан 137 фоизни ташкил этди [2]. 2022 йилнинг биринчи ярмида “UZ” домен ҳудудида 83 та аниқланган ҳужумлар рўй берди. Давлат органларининг веб-сайтларида шу ярим йилда 23 та ахборот хавфсизлигига ҳамла қилинди [3].

Телеграм мессенжерининг россиялик фойдаланувчиларига таркибида зиёнкор дастурий таъминот мавжуд бўлган оммавий тарқатмалар келмоқда. Бу тўғрида “Касперский лабораторияси” огоҳлантирди. Хакерлар коронавирус тарқалганлигидан фойдаланиб компьютерларга ҳужум қилишни кучайтирди. Бундай хабарлар кўпинча номаълум жўнатувчилардан келади ва уларга бириктирилган файллар кўпинча хитойча номланган. Бу иероглифлар асосан “Салом”, “Тўловни қабул қилиб олинг” каби маъноларни англатади. Бундай файллар троян бўлиб, киберхавфсизлик бўйича мутахассислар уларни Gh0st вируслар оиласига мансуб, деб ҳисоблашади.

Агар Телеграм мессенжери (Телеграм Десктоп иловаси) орқали келган шундай бирор файлни Windows тизимли компьютерда очсангиз, троян операцион тизимга тушади ва чуқур ўрнашиб олади. Мазкур дастурий таъминот Remote Admin Tool жиҳозларининг деярли барча жиҳозлари билан куролланган. “Касперский лабораторияси” экспертларининг таъкидлашларича, бундай турдаги вируслар энг хавфли ҳисобланади; зеро, улар хакерларга компьютерингизга киришнинг кенг имкониятларини тақдим этади. Бошқача айтганда, бу вирус компьютер бошқарувини ҳеч бир чекловсиз бошқариш ҳуқуқини қўлга киритади. У тугмачаларнинг босилишини, сичқонча билан чертишларни ҳисоблашга қодир. Вирус яратувчисига киберҳужум қурбонининг компьютерига масофадан уланиш имконини беради. Иловаларнинг паролларини ўғирлайди ва веб-камера билан ҳам ишлай олади. Телеграм орқали троянлар ҳужуми 2020 йилдаёқ бошланган, аммо айнан ҳозирга келиб улар кенг тарқалмоқда. Мутахассислар мессенжернинг Android, iOS ёки macOS тизимларига мўлжалланган клиентларида бундай хавф борлигини айтишмаяпти. Троянлар асосан Windows тизимли ноутбук ва компьютерларга таҳдид туғдирмоқда. Демак, ушбу қурилмалар эгалари янада эҳтиёткор бўлишлари лозим. Бунда бегона кишилардан ёки каналлардан келган, гуруҳларда тарқатилган, ғалати номлардаги файлларни компьютерда умуман очмаслик тавсия этилади [4].

Ҳозирги даврда кибер хавфсизлик таҳдидини текшириш мақсадида ВПНПро компанияси мутахассислари Андроид операцион тизими учун ишлаб чиқилган оммабоп антивирус-иловалардан ўн бештасини текшириб кўрди. Маълум бўлишича, улардан айримлари ўзининг ишлаши учун умуман керак бўлмайдиган функцияларга киришга ҳам руҳсат олар экан. Тест қилиб

кўрилган 15 та антивирус ва тозаловчи иловадан олтитаси смартфоннинг камераси ва микрофонига, кўнғироқларга, СМС-хабарларга ва ички хотирага кириш учун рухсат сўраши аниқланган. Буларга кириш имконига эга бўлгач, мазкур дастурлар фойдаланувчининг шахсий маълумотларини кузатишлари ва ўз ишлаб чиқувчиларига (эгаларига) жўната бошлайди. Куйида ана шу потенциал хавфли тозаловчи иловалар рўйхати келтирилган: Security Master (500 миллион марта ўрнатиб олинган), Antivirus Free 2019 (10 миллион марта ўрнатиб олинган), Virus Cleaner 2019 (50 миллион марта ўрнатиб олинган), Max Security Virus Cleaner, Antivirus, Cleaner (50 миллион марта ўрнатиб олинган), Super Phone Cleaner, Virus Cleaner, Phone Cleaner (50 миллион марта ўрнатиб олинган), Clean Master (1 миллиард марта ўрнатиб олинган).

Тўғри, компания экспертлари буларнинг ҳақиқатан ҳам жосуслик қилаётганига тўғридан-тўғри далил топа олиши қийин. Аммо, антивируслар амалда ўзларига керак бўлмаган имкониятларга ҳам рухсат олишларининг ўзиёқ уларнинг тизим имкониятларини суиистеъмол этишларидан дарак беради. Бунда шахсий маълумотларнинг ниқобланган ҳолда узатилиши учун барча имкониятлар мавжуд.

ВПНПро мутахассислари текширув натижаларини Googleга тақдим этгач, қидирув гиганти уларни Play Marketдан ўчириб ташлаган. Бироқ улар шу пайтгача ўрнатиб олган фойдаланувчиларнинг қурилмаларида, шунингдек бошқа иловалар дўконларида йўқолмаган ва қолган. Шуларни эътиборга олиб, ВПНПро экспертлари фақат нуфузли ва ишончли (масалан, Аваст, Авира, “Касперский лабораторияси” ва Dr.Web тақдим этаётган) антивируслардан фойдаланишни тавсия қилишмоқда[5].

Билл Гейтс давлатлар ҳукуматлари инсониятни кутаётган яна бир хавф – биологик террорчиликка қарши курашга маблағлар йўналтириш долзарб масала эканлиги масаласини кўтарди. “Business Insider” нашри хабарига кўра, бу фикрни у Хавфсизлик бўйича Мюнхен анжуманида айтди. Гейтснинг айтишича, замонавий шароитларда ғараз ниятли одамлар хавфли вирусларни, масалан, грипп ёки чечакнинг қирғин келтирувчи версиясини яратиши мумкин. Унинг фикрича, “кейинги эпидемиянинг сабаби террорчилик мақсадида биоинженерия усуллари билан хавфли вируслар яратилиши бўлиши мумкин”[6].

2019 йил 27 мартда, яъни орадан икки йил ўтгач Ўзбекистон жаҳон киберавфсизлик рейтингида 52-ўринни эгаллади. Очиқ манбаларни ўрганиш, MSE тузилмасида турли ташкилотлар билан ўзаро ҳамкорлик қилиш, Ўзбекистон Республикасининг халқаро муносабатларини, жумладан, киберхавфсизлик масалаларида кенг кўламли ишлари, мамлакатимиз жаҳон ҳамжамиятида ижобий баҳо берилди ва эътироф этилди [7].

Мамлакатларнинг киберхавфсизликка бўлган мажбуриятини баҳоловчи Global Cybersecurity Index (GCI)нинг 2021 йил 10 октябрдаги маълумотиغا биноан Ўзбекистон глобал киберхавфсизлик бўйича 194 мамлакат рейтингида 70-ўринни эгаллаб, унинг индекси максимал 100 баллдан 71,11 баллни ташкил этди. Қайд этилишича, мамлакат куйидаги бешта асосий йўналиш бўйича 20

баллик системада баҳоланган: қонуний чоралар, техник чоралар, ташкилий чоралар, салоҳиятни ривожлантириш чоралари, ҳамкорлик чоралари. Ўзбекистон энг юқори балли ҳуқуқий чоралар сегментида олди (19,27 балл), энг пасти балли эса ташкилий чораларга тегишли (10,05 балл) бўлди. Шунингдек, мамлакатга техник чора-тадбирлар соҳаси учун 12,56 балл, салоҳиятни ривожлантириш чора-тадбирлари учун 15,68 ва ҳамкорлик чоралари учун эса 13,56 балл берилди. Таъкидланишича, Марказий Осиё давлатлари орасида киберхавфсизлик бўйича Ўзбекистон Қозоғистондан (рейтингда 31-ўринда) кейин иккинчи ўринни қайд этган (Қирғизистон 92-ўринни, Тожикистон 138-ўринни, Туркменистон эса 144-ўринни эгаллади). АҚШ (100 балл) биринчи, Буюк Британия ва Саудия Арабистони (ҳар бири 99,54 балл) иккинчи, Эстония (99,48 балл) учинчи ўринни олиб кучли учликни ташкил қилди. Рейтингда охириги ўрин Шимолий Кореяга тегишли бўлди (1,35 балл)[8].

“Янги Ўзбекистоннинг 2022-2026 йилларга мўлжалланган тараққиёт стратегиясида 2022 йил октябрга қадар “2023-2026 йилларга мўлжалланган Ўзбекистон Республикасининг киберхавфсизлик стратегияси”ни ишлаб чиқиш вазифаси қўйилди. Унда, “UZ№ домен зонаси Интернет-маконининг киберхавфсизлигини таъминлашнинг асосий йўналишлари ҳамда электрон ҳукумат, энергетика, рақамли иқтисодиёт тизимлари ва муҳим ахборот инфратузилмасига тааллуқли бошқа йўналишларни ҳимоя қилиш бўйича комплекс вазифалар белгиланади. Шунингдек, кибержиноятчилик учун жиноий жавобгарликни қайта кўриб чиқиш кўзда тутилган. Шу билан бирга, ҳужжатда ахборот майдонидаги киберхужум ва таҳдидларни мониторинг қилиш тизимини янада такомиллаштириш вазифалари белгиланди. Унга биноан киберхавфсизликнинг Ягона тармоғининг техник инфратузилмасини кенгайтириш, рибернетикада инновациялар ИТ-парки” фаолиятини янада жадаллаштириш, ИТ-паркнинг ҳудудлардаги рақамли технологиялар ўқув марказлари негизида ёшларни киберхавфсизлик асослари бўйича ўқитилишини таъминлаш ҳамда ҳар йили талаба ва ўқувчилар орасида киберхужумлар аниқлаш бўйича республика миқёсида конкурслар ўтказишни назарда тутиш қайд этилди [9].

Президент Ш.М.Мирзиёев ташаббуси билан 2022 йил 21 апрелда парламент томонидан “Киберхавфсизлик тўғрисида”ги қонуннинг қабул қилиниши мамлакатда ахборот хавфсизлигини таъминлаш соҳасидаги катта бурилиш бўлди. Мазкур қонуннинг қабул қилиниши мамлакатда ахборот-коммуникация воситаларини ички ва ташқи киберхужумлардан ҳимоя қилиш соҳасининг ҳуқуқий асосларини ҳар томонлама мустаҳкамлади. Қонун 8 та боб ва 40 та моддадан иборат бўлиб, унда мамлакатнинг киберхавфсизлигини таъминлашнинг қуйидаги асосий принциплари белгиланди: қонунийлик, кибермаконда шахс, жамият ва давлат манфаатларини ҳимоя қилишнинг устуворлиги, киберхавфсизлик соҳасини тартибга солишга нисбатан ягона ёндашув, киберхавфсизлик тизимини яратишда маҳаллий ишлаб чиқарувчилар иштирокининг устуворлиги, Ўзбекистон Республикасининг

киберхавфсизликни таъминлашда халқаро ҳамкорлик учун очиклиги. Шунингдек, қонунда Киберхавфсизлик соҳасидаги ягона давлат сиёсатини Ўзбекистон Республикаси Президенти белгилаши мустаҳкамланди. Шу билан бирга, Ўзбекистон Республикаси Давлат хавфсизлик хизмати киберхавфсизлик соҳасидаги ваколатли давлат органи эканлиги белгиланди. Қонунга биноан, киберхавфсизлик субъектлари томонидан киберхавфсизлик ходисаларига нисбатан чоралар кўриш дастурий таъминотдаги ва курилмалардаги заифликларни ҳамда хатоликларни бартараф этиш, зарарли дастурларни йўқ қилиш, уларнинг тарқалишини чеклаш, киберхужумлар манбаини техник жиҳатдан чеклаш, ахборотлаштириш объектларини мавжуд кибертахдидлардан ажратиб қўйиш, ҳуқуқни муҳофаза қилувчи органларга киберхавфсизлик ходисалари тўғрисида маълумотлар тақдим этиш каби шаклларда амалга оширилиши мумкин [10].

Хулоса қилиб айтганда, 2021-2022 йилларда мамлакатда жамият барқарорлигини таъминлашнинг муҳим соҳаси – ахборот хавфсизлигини мустаҳкамлаш ва такомиллаштириш соҳасида чуқур ислохотлар амалга оширилди. Бу албатта, мамлакатда Янги Ўзбекистон ва учинчи Реннесанс пойдеворини шакллантириш ислохотларининг муҳим бир қисми эди. Бу даврда “Киберхавфсизлик маркази” давлат унитар корхонасини ташкил этилиши, “Киберхавфсизлик тўғрисида”ги қонунни қабул қилиниши, ахборот хавфсизлигига оид технологияларнинг янгиланиши ва такомиллаштирилиши натижасида киберхужумлар ҳамласига нисбатан тўсиқлар қўйилди, жамият барқарорлиги ва хавфсизлиги таъминланди. Шунингдек, ахборот хавфсизлигининг истиқболларини янада яхшилаш мақсадида бу соҳа моддий техника базасини ривожлантирилиши – бу соҳани янада ривожланиб бораётгани далилидир.

#### **Адабиётлар:**

1. Кейсы кибератак в Центральной Азии. Кыргызстан и Узбекистан. 23-03 г. // <https://mediasabak.org/ru/news/241/>.
2. Кибербезопасность 2022: обеспечение цифровой безопасности/. 30.06.2022 и // <https://review.uz/post/kiberbezopasnost-2022-obespechenie-cifrovoy-bezopasnosti/>.
3. Статистика проверок, по состоянию на I- полугодие 2022 года:// <https://csec.uz/ru/>.
4. Касперский лабораторияси» огоҳлантиради: “Telegram энди хавфсиз эмас!” // <https://www.terabayt.uz/post/kasperskiy-laboratoriyasi-ogohlantiradi-telegram-endi-xavfsiz-emas>.
5. Смартфонингизда жосуслик қилаётган олтига антивирус. // <https://www.terabayt.uz/post/smartfoningizda-josuslik-qilayotgan-oltita-antivirus>.
6. Билл Гейтс: “Дунёни биотеррор хавфи кутмоқда!” // <https://www.terabayt.uz/post/bill-gejts-dunyonibioterror-xavfi-kutmoqda>.
7. Собиров Ў. Глобал киберхавфсизлик индекслари ва Ўзбекистоннинг рейтинги: кучли ўсиш. 3.04.2019 й. // <https://ictnews.uz/03/04/2019/global-cybersecurity-index/>.

8. Ўзбекистон киберхавфсизлик бўйича мамлакатлар рейтингида 70-ўринни эгаллади. 12 октябрь 2021 й.// <https://uznews.uz/posts/534>.
9. Ўзбекистонда киберхавфсизлик стратегияси ишлаб чиқилади. 03.01.2022 й.//<https://xabar.uz/post/ozbekistonda-kiberxavfsizlik-strat>.
10. Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги қонуни. 15.04.2022 й.// Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон.