КИБЕРТОВЛАМАЧИЛИКНИНГ ЎЗИГА ХОС ЖИҲАТЛАРИ ИЛМИЙ ТАҲЛИЛИ

Каймходжаев Ойбек Абдукаримович
Мустақил изланувчи

Аннотация. *Мазкур мақолада ахборот технологияларининг жадал ривожланиши шароитида кибертовламачилик жиноятларининг келиб чиқиш сабаблари, турлари ва уларнинг жамият барқарорлигига таъсири илмий-амалий жиҳатдан таҳлил қилинган. Ўзбекистон Республикасида кибертовламачилик жиноятларининг статистик кўрсаткичлари асосида уларнинг ўсиш динамикаси ҳамда ҳудудий хусусиятлари ўрганилган. Шунингдек, кибертовламачиликка қарши курашишнинг ҳуқуқий, ташкилий ва техник механизмларини такомиллаштириш бўйича илмий асосланган таклифлар илгари сурилган.*

Калит сўзлар: *кибержиноятчилик, кибертовламачилик, рақамли технологиялар, ахборот хавфсизлиги, киберхавфсизлик, жиноятчиликка қарши кураш.*

НАУЧНЫЙ АНАЛИЗ СПЕЦИФИЧЕСКИХ ОСОБЕННОСТЕЙ КИБЕРВЫМОГАТЕЛЬСТВА

Аннотация. *В данной статье в условиях стремительного развития информационных технологий с научно-практической точки зрения проанализированы причины возникновения кибервымогательства, его основные виды, а также влияние данных преступлений на устойчивость общества. На основе статистических показателей Республики Узбекистан исследованы динамика роста*

кибервымогательных преступлений и их территориальные особенности. Кроме того, выдвинуты научно обоснованные предложения по совершенствованию правовых, организационных и технических механизмов противодействия кибервымогательству.

Ключевые слова: *киберпреступность, кибервымогательство, цифровые технологии, информационная безопасность, кибербезопасность, противодействие преступности.*

SCIENTIFIC ANALYSIS OF THE SPECIFIC FEATURES OF CYBER EXTORTION

Abstract. *This article provides a scientific and practical analysis of the causes of cyber extortion, its main types, and the impact of such crimes on societal stability in the context of the rapid development of information technologies. Based on statistical data from the Republic of Uzbekistan, the dynamics of cyber extortion crimes and their territorial characteristics are examined. In addition, scientifically grounded proposals are put forward to improve legal, organizational, and technical mechanisms for countering cyber extortion.*

Keywords: *cybercrime, cyber extortion, digital technologies, information security, cybersecurity, crime prevention.*

Сўнгги йилларда рақамли технологияларнинг барча соҳаларга чуқур кириб бориши жамият тараққиёти учун янги имкониятлар яратаётган бўлса-да, айни пайтда ахборот технологияларидан фойдаланиб содир этиладиган жиноятлар сонининг ортишига ҳам сабаб бўлмоқда. Айниқса, кибертовламачилик жиноятлари шахс, жамият ва

давлат манфаатларига жиддий таҳдид солаётган долзарб муаммолардан бирига айланди.

Кибертовламачиликнинг асосий хавфли жиҳати унинг яширинлиги, трансчегаравий хусусияти ҳамда жиноят содир этган шахсларни аниқлаш ва жавобгарликка тортишнинг мураккаблиги билан изоҳланади. Шу боис ушбу жиноят турини илмий-амалий жиҳатдан чуқур таҳлил қилиш ва самарали қарши курашиш механизмларини ишлаб чиқиш долзарб аҳамият касб этади.

Илмий манбаларда кибержиноятчилик компютерлар, компютер тармоқлари ёки ахборот тизимларидан фойдаланган ҳолда содир этиладиган жиноятлар мажмуи сифатида талқин этилади[1]. Кибержиноятчилик алоҳида шахслар, ташкилотлар ва ҳатто ҳукуматларга таъсир қилиши мумкин ва у кўпинча рақамли маълумотлар ва ресурсларга рухсатсиз кириш, бузиш ёки ўғирлашни ўз ичига олади. Замонавий жамиятда интернет ва технологияларга қарамлик ортиб бораётгани сабабли, кибержиноятчилик жиддий муаммога айланмоқда.

Кибертовламачилик эса ушбу жиноятларнинг мустақил ва тез ўсиб бораётган тури бўлиб, электрон алоқа воситалари орқали таҳдид қилиш, қўрқитиш ёки шантаж йўли билан моддий ёки номоддий манфаат олишга қаратилган ноқонуний ҳаракатларни ўз ичига олади. Кибертовламачиликнинг ўзига хос хусусияти шундаки, жиноятчилар аксарият ҳолларда анонимликдан фойдаланади, криптовалюталар орқали тўлов талаб қилади ва миллий юрисдикциядан ташқарида фаолият олиб боради.

Ўзбекистон Республикаси Статистика қўмитасининг маълумотларига кўра, ахборот ва алоқа хизматлари ҳажми 2021–2024

[1] https://www.academia.edu/107947985/Cyber_Crime

йиллар давомида сезиларли даражада ўсган. 2024 йилда интернет тармоғига уланган абонентлар сони 32 миллион нафардан ошгани аҳолининг рақамли муҳитга тобора кўпроқ жалб этилаётганини кўрсатади[2].

Шу билан бирга, 2024 йилда ахборот технологиялари ёрдамида 61 мингдан ортиқ жиноят содир этилган бўлса, 2025 йилда ушбу кўрсаткич 25,4 фоизга ошган[3]. Бу кибертовламачилик жиноятларининг барқарор ўсиш тенденциясига эга эканлигини тасдиқлайди.

Жиноятчиликнинг экспоненсиал ўсиши билан кибержиноятчилик дунёдаги энг кенг тарқалган жиноятлар орасида коррупцияси ва гиёҳванд моддалар савдосидан кейин учинчи ўринни эгаллади. Ушбу жиноятни кенг тарқалишига сабаб интернет фойдаланувчиларининг қарийб 2/3 қисми кибержиноятларга дучор бўлмоқда, яъни уларнинг шахсий маълумотлари ўғирланмоқда ёки хавф остида қолаётганлиги, кибержиноят содир этган шахснинг қамоққа тушиш эҳтимоли жуда пастлиги, кибержиноят содир этаётган хакерларнинг аксарияти бу ҳақда билади ва ўз шахсиятини сир тутади, шунинг учун уларни кузатиш қийин.

Товламачилик дастурлари – бу кибержиноятчиликнинг тез ўсиб бораётган тури бўлиб, бундай турдаги кибержиноятларни амалга ошириш учун маҳсулот ва хизматларни сотадиган 6000 дан ортиқ онлайн платформалар мавжуд[4].

[2] https://api.siat.stat.uz/media/uploads/sdmx/sdmx_data_1208.pdf
[3] IIV HSvaTHMBMning 26.12.2025-yildagi ma‘lumotlari asosida.
[4] Tanishq Verma, Dhruv Garg. “Understanding Cybercrime and its Consequence Worldwide”. file:///C:/Users/User/Downloads/Understanding_Cybercrime_and_its_Consequ.pdf

Таҳлиллар шуни кўрсатадики, кибертовламачилик ўсиб бормоқда ва келгуси ўн йилликларда жадал суръатлар билан ўсиши кутилмоқда. Таъқиб ва товламачилик жисмоний дунёда ҳам, рақамли соҳада ҳам шахслар, ташкилотлар ёки субъектларга қаратилган мажбурий ёки таҳдидли хатти-ҳаракатларни ўз ичига олади. Компютер технологияларидан фойдаланган ҳолда содир этилганда, бу "кибер таъқиб" ёки "кибер товламачилик" деб аталади. Бундай ҳолларда жиноятчилар ўз қурбонларини қўрқитиш, таҳдид қилиш ёки мажбурлаш мақсадида шахсий фойда ёки зарар етказиш учун электрон алоқадан фойдаланадилар.

2024 йилги маълумотларга кўра *100 та уй хўжалигига тўғри келадиган мобил телефонлар* сони ***356 та***ни ташкил этиб[5], хонадоннинг 3 нафар оила аъзоси мобил телефондан фойдаланиши, уларнинг ёши ва маълумоти билан боғлиқ турли фарқлар кибертовламачилар учун қулай шароит яратади.

Экспертларнинг фикрича, кибержиноятчиликнинг ажралиб турадиган хусусияти унинг табиий географиядан ажралиб туришидир[6]. Жумладан, кибержиноятчиликнинг ҳудудий тақсимоти яхши ҳужжатлаштирилган бўлса-да, кибержиноятчиликнинг географик маконда қандай ўзгариши масаласи ҳали ҳам ўрганилмаган. Чекланган миқдордаги тадқиқотлар кибержиноятчиликни мамлакатлар ёки давлатлар каби кенг агрегация даражаларида ўрганган[7].

Кўплаб ҳуқуқни муҳофаза қилувчи органлар, жумладан ички ишлар органларининг соҳавий хизмат ходимлари кибертовламачиликка қарши

[5] https://api.siat.stat.uz/media/uploads/sdmx/sdmx_data_568.pdf
[6] https://www.academia.edu/143058333/Cybercrime_vs_Non_Cybercrime_Do_Crime_and_Victimization_Differ_by_Location
[7] Ўша ерда.

курашишда ўзларини алоқадор эмасликларини рўкач қилишлари, ушбу жиноят турларига алоҳида бўлинмалар қарши курашиши кераклиги каби тушунчаларнинг мавжудлиги жиноятчиликка қарши курашишда бир қатор қийинчиликлар, жумладан жабрланувчилар сонининг ошиши, жиноятни фош этиш даражасининг пастлиги, шу билан биргаликда жабрланувчиларнинг географик минтақалар бўйича ҳисоботларида нотекисликларни келтириб чиқариши мумкин.

Чунки, кибертовламачиликка қарши курашишда амалга оширилиши лозим бўлган ташкилий чора-тадбирлар тўғри йўлга қўйилмаганлиги жиноятчилик статистикасининг ўсишига олиб келади.

2024 йилда мобил алоқа тизимига уланган абонент радиостанциялари сони, жисмоний шахсларда 100 та ўртача доимий аҳолига нисбатан ***80,8 нафар*** бўлса, *интернет тармоғига уланган абонентлар сони* ***80,1 нафар***ни, яъни ***99,1 фоиз*** абонент радиостанциялари интернет тармоқларига уланган[8].

Олимларнинг фикрича, нокибержиноятчилик одатда географик жиҳатдан чекланган деб тушунилади, кибержиноятчилик эса **бундай эмас.** Нокибержиноятчилик шаҳар атрофидаги ёки қишлоқ жойларига қараганда шаҳарларда кўпроқ учрайди. Бироқ, кибержиноятчилик ушбу фазовий қонуниятга бўйсуниши шарт эмас. Тўғридан-тўғри эмпирик далиллар мавжуд бўлмаса-да, баъзи олимлар кибержиноятчилик шаҳар атрофи ва қишлоқ жойларига қараганда шаҳар жойларида кўпроқ тарқалган бўлиши мумкинлигини тахмин қилишади, чунки шаҳар атрофи ва қишлоқ жойларида жойлашган ҳуқуқни муҳофаза қилувчи органларида ресурсларнинг

[8] https://api.siat.stat.uz/media/uploads/sdmx/sdmx_data_417.pdf

чекланганлиги каби омиллар мавжуд[9]. Аксарият ҳолларда ташқи хавфлар манбаи Ўзбекистон Республикаси қонунчилиги юрисдикцияси доирасига кирмайди. Бу эса ҳуқуқий чоралар тизимини қўллашни муайян даражада мураккаблаштиради. Кибержиноятчилар, одатда, миллий чегараларни четлаб ўтган ҳолда, жаҳон тармоғига уланган ҳар қандай комютерга, электрон дастурга ҳужум қилади.

Жаҳон тажрибаси ва миллий амалиёт таҳлили асосида кибертовламачилик қуйидаги асосий турларга ажратилди:

Кибербуллинг – ижтимоий тармоқлар орқали шахсни, айниқса вояга етмаганларни таъқиб қилиш, ҳақоратлаш ва туҳмат қилишдир. Ижтимоий тармоқлар, электрон почта ёки хабар алмашиш иловалари каби рақамли воситалар орқали шахсларни, айниқса вояга етмаганларни таъқиб қилиш саналиб, асосан ахборот технологиялари ёрдамида ижтимоий тармоқларда туҳмат ва ҳақорат қилиш билан боғлиқ ҳаракатлар бўлиб, ўтган йилга нисбатан ўзини ўзи ўлдиришга ундаш ***100 фоиз,*** туҳмат қилиш ***53 фоиз,*** ҳақорат қилиш эса ***52,2 фоиз***га ошганлиги ҳам бунинг яққол мисоли бўла олади[10].

Онлайн таҳдидлар – жисмоний ёки маънавий зарар етказиш билан қўрқитиш орқали талаб қўйишдир. Жисмоний шикаст етказиш ёки оммавий камситиш билан таҳдид қилиб, жабрланувчига таҳдидли хатлар ёки хабарлар юбориш, пул, махфий маълумотлар ёки бошқа шаклдаги талабларни талаб қилиш ҳам инсонларга бир қатор жиддий эмотсионал хатарлар келтириб чиқариб, ўтган йилга нисбатан шахснинг шаънини ва қадр-қимматини камситувчи ҳамда инсон ҳаётининг сир тутиладиган

[9] https://www.academia.edu/143058333/Cybercrime_vs_Non_Cybercrime_Do_Crime_and_Victimization_Differ_by_Location

[10] IIV HSvaTHMBMning 26.12.2025-yildagi ma‘lumotlari asosida.

томонларини акс эттирувчи маълумотларни ошкор қилиш ***72,2 фоиз***га ошган [11].

Қасоскор порнография – шахснинг розилигисиз интим материалларни тарқатиш орқали шантаж қилиш. Одамнинг розилигисиз унинг беҳаё расмлари ёки видеоларини тарқатиш, одатда жабрланувчини камситиш ёки товламачилик мақсадида содир этилади. Таҳлилларга кўра порнографик маҳсулотни тайёрлаш, олиб кириш, тарқатиш, реклама қилиш, намойиш этиш ўтган йилга нисбатан ***14,3 фоиз***га ошган[12].

Ransomware орқали товламачилик – ахборотларни шифрлаб, уларни тиклаш учун тўлов талаб қилиш. Кибертовламачи дастурий таъминот орқали зарарли дастурни жабрланувчининг маълумотларига юбориб, уни шифрлайди ва бузғунчи шифрни очиш калити учун тўлов талаб қилади. Таҳлилларга кўра, ўтган йилга нисбатан зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш ***72,3 фоиз***, шахсга доир маълумотлар тўғрисидаги қонунчиликни бузиш ***50 фоиз***, товламачилик ***71,1 фоиз***га ошган[13].

Таҳлилларга кўра кибертовламачиликнинг кенг тарқалишига қуйидаги омиллар таъсир кўрсатмоқда:

интернет муҳитидаги нисбий анонимлик (интернет томонидан тақдим этилган нисбий анонимлик кибержиноятчиларга аниқланишдан қўрқмасдан ишлашни осонлаштиради. Бу анонимлик одамларни ноқонуний фаолиятга ундаши мумкин. Айниқса, *хакерлар ҳужумлар учун сунъий интеллектдан максимал даражада фойдаланаётганликлари ҳам* кибертовламачиликнинг анонимлигини таъминлайди)[14];

[11] Ўша ерда.
[12] Ўша ерда.
[13] Ўша ерда.
[14] https://www.academia.edu/107947985/Cyber_Crime

юқори молиявий фойда олиш имконияти (кўплаб кибержиноятчилар молиявий рағбатлар билан рағбатлантирилади. Хакерлик, шахсни ўғирлаш ва онлайн фирибгарлик жисмоний иштироксиз ёки қарама-қаршилик хавфисиз пул олиш имкониятларини тақдим этади);

қора тармоқда техник воситаларнинг осон топилиши (қора тармоқда бузиш воситалари, дарсликлар ва ресурсларнинг кенг тарқалиши туфайли техник билимлари чекланган одамлар кибержиноятчиларга айланиши мумкин. Кириш тўсиғи анъанавий жиноий фаолиятга қараганда пастроқ);

рақамли маконнинг глобал хусусияти (рақамли оламнинг ўзаро боғлиқлиги кибержиноятчиларга бутун дунё бўйлаб қурбонларни нишонга олиш имконини беради. Бу глобал қамров жиноий фаолият учун кўпроқ имкониятлар яратади);

қонунчилик ва ҳуқуқни қўллаш механизмларининг етарли даражада ривожланмаганлиги (кибержиноятчилик қонунчилиги ва ҳуқуқни муҳофаза қилиш имкониятлари кўпинча кибержиноятчилар томонидан қўлланиладиган тез ривожланаётган техника ва технологиялардан орқада қолмоқда. Бу жиноятчиларнинг жазосиз фаолияти учун қулай муҳит яратади).

Бундан ташқари, 5G технологиясининг жорий этилиши ҳам киберхавфларнинг янги кўламини шакллантирмоқда. Бутун дунё бўйлаб 5G тўлиқ жорий этилгандан сўнг, кўпроқ нарсалар интернети қурилмалари Wi-fi йўналтиргичга уланиш ўрнига тўғридан-тўғри 5G тармоғига уланади, бу эса уларни ҳужумларга янада заифроқ қилади.

Маълумотларига кўра, алоқа корхоналарининг аҳолига алоқа хизматидан тушган тушуми таркибида мобил алоқа хизматларининг

улуши 33,9 фоиз, аҳолига алоқа хизматидан тушган тушуми таркибида маълумот узатиш тармоғи “Интернет”ни қўшган ҳолда хизматининг улуши 64,6 фоиз ташкил этиб, ушбу кўрсатгич 2021 йилга нисбатан 30,3 фоиз ошган[15].

Таҳлиллар Навоий, Сурхондарё, Жиззах вилоятлари ҳамда Тошкент шаҳрида кибертовламачилик билан боғлиқ жиноятлар сони сезиларли ошганини кўрсатмоқда. Бу ҳолат аҳоли сонининг кўпайиши ва ижтимоий тармоқлардан фойдаланиш даражасининг ортиши билан бевосита боғлиқ.

Навоий вилоятида 91,3 фоиз, Сурхондарё вилоятида 82,9 фоиз, Жиззах вилоятида 74,1 фоизга ошган бўлиб, сон жиҳатдан Тошкент шаҳарида икки баробарга, Самарқанд вилоятидан уч баробарга, Фарғона вилоятида икки ярим баробарга ўсганлиги ушбу ҳудудлар аҳолисининг кўпайиб бораётганлиги ҳамда ижтимоий тармоқлардан кенг кўламда фойдаланаётганлиги сабабли юз бермоқда.

Жумладан, аҳоли сони 2021 йилдан буён Тошкент шаҳрида 15,4 фоиз, Сурхондарё вилоятида 8,9 фоиз, Жиззах вилоятида 8,2 фоиз, Самарқанд вилоятида 8,1 фоиз, Фарғона вилоятида 7,8 фоиз, Навоий вилоятида 7,5 фоиз кўпайганлиги муҳим аҳамият касб этади[16].

Илмий манбаалар таҳлилига кўра сўнгги йилларда товламачи дастурлардан фойдаланувчи жиноятчилар қурбонларни тўловга мажбурлаш учун тобора шафқатсизроқ усулларни қўлламоқда. Икки босқичли товламачилик кенг тарқалган стратегияга айланди. Бунда жиноятчилар нафақат маълумотларни шифрлайди, балки тўлов амалга оширилмаса, махфий ахборотни ошкор қилиш билан таҳдид солади.

[15] https://api.siat.stat.uz/media/uploads/sdmx/sdmx_data_345.pdf
[16] https://stat.uz/uz/rasmiy-statistika/demography-2

Бундай ёндашув қурбонларга босимни кучайтиради, чунки ошкоралик ва ҳуқуқий оқибатлар хавфи тўловни амалга ошириш шошилинчлигини оширади. Баъзи гуруҳлар мижозлар, ҳамкорлар ёки учинчи шахслар каби қўшимча манфаатдор томонларга қаратилган уч босқичли товламачиликни қўллаш орқали янада илгарилаб кетди. Бундай ҳолатларда жиноятчилар бир нечта томонлардан тўловларни талаб қилишлари мумкин, бу эса уларнинг фойдасини ва таъсирини янада кучайтиради[17].

Жаҳон ҳисоботига кўра, Шимолий Америка, Европа, Марказий Осиё, Шарқий Осиё ва Тинч океани минтақаси, Жанубий Осиё, Лотин Америкаси ва Кариб ҳавзасидаги кибержиноятлар сони баҳоланмоқда. Ҳисоботда ушбу ҳудудларда содир бўлаётган кибержиноятлар сони тегишли ҳукуматлар томонидан қўлланилаётган киберхавфсизлик чораларига боғлиқлиги тавсифланиб, башорат қилинган. Бу чоралар ҳуқуқий, техник, ташкилий тадбирлар ҳамда салоҳиятни оширишни ўз ичига олади. Кибержиноятчилик натижалари уч даражага ажратилган: юқори, ўрта ва бошланғич. Юқори даражага кучли киберхавфсизлик ва ривожланган рақамли иқтисодиётга эга мамлакатлар киради. Ўрта даража ривожланаётган ва киберхавфсизлигини мустаҳкамлаётган мамлакатлардан иборат. Бошланғич даража эса киберхавфсизликнинг асосий даражасига эга мамлакатлардир[18]. Баъзи мамлакатлар киберҳужумларга жиддий равишда мўлжалланган. Улар орасида:

[17] Managt Socio Human, International Res Jour. “Ransomware Attacks: Trends, Impacts, and Prevention Strategies”. Isarasolutions, 2025.

[18] Tanishq Verma, Dhruv Garg. “Understanding Cybercrime and its Consequence Worldwide”. file:///C:/Users/User/Downloads/Understanding_Cybercrime_and_its_Consequ.pdf

Бразилия – тадқиқотга кўра, Бразилия киберҳужумларнинг иккинчи йирик манбаи ҳисобланади.

Япония – Илгари Япония алоқа/тил тўсиғи туфайли кибержиноятчиликдан унчалик зарар кўрмаган. Бироқ, ҳозирги кунда банкларга қарши ҳужумлар сони тез суръатларда ортиб бормоқда.

Шунигдек, кибертовламачиликка қарши курашишда *халқаро тажрибалар ўрганилганда*, **Қўшма Штатларда** Интернет жиноятлари устидан шикоят қилиш маркази (IS3) кибержиноятлардан жабрланганлар ва ҳуқуқни муҳофаза қилиш органлари ўртасида воситачилик қилади. У статистик маълумотларни тўплайди ва ҳар йили бутун мамлакат бўйлаб кибержиноятчилик кўламини ёритувчи ҳисоботларни эълон қилади[19].

Юқоридагилар таҳлили асосида кибертовламачиликка қарши курашишда қуйидаги чора-тадбирларни амалга ошириш таклиф этилади:

маълумотларнинг мунтазам захира нусхаларини яратиш, яъни товламачилик дастурлари ҳужуми юз берганда жисмоний ва юридик шахслар иш фаолиятининг узлуксизлигини таъминлаш учун муҳим маълумотларнинг тез-тез автоном захира нусхаларини яратишни йўлга қўйиш;

дастурий таъминот ва операцион тизимларни доимий янгилаш. Хусусан, дастурий таъминот ва операцион тизимларни ўз вақтида янгилашни таъминлаш, товламачилик дастурлари фойдаланиши мумкин бўлган заифликларни бартараф этиш учун автоматлаштирилган тизимларни жорий этиш;

[19] Demir, Mustafa. “Cybercrime vs. Non-Cybercrime: Do Crime and Victimization Differ by Location.” Journal of Crime and Justice , 2025. https://www.academia.edu/143058333/Cybercrime_vs_Non_Cybercrime_Do_Crime_and_Victimization_Differ_by_Location

фишинг ва ижтимоий инженерияга қарши ходимларни ўқитиш, жумладан ходимларни ўқитиш орқали фишинг электрон хатларини аниқлашни ва улар ҳақида хабар бериш ўрганиш *(чунки булар товламачилик дастурларининг тарқалишидаги асосий восита ҳисобланади);*

сунъий интеллект асосидаги IDS ва EDR тизимларини жорий этиш. Товламачилик дастурларни реал вақт режимида аниқлаш ва бартараф этиш учун сунъий интеллектга асосланган кириш-чиқишни назорат қилиш тизимларини (IDS) жорий этиш *(Интрусионликни аниқлаш тизими (IDS) тармоқ трафигини назорат қилади ва шубҳали фаолиятни кузатиб боради ва тизим ёки тармоқ администраторини огоҳлантиради. Баъзи ҳолларда IDS фойдаланувчи ёки манба* IP-манзилини *тармоққа киришни блокировкалаш каби хатти-ҳаракатларни амалга ошириб, аномал ёки ёвуз трафикка жавоб бериши мумкин)* ҳамда қурилмаларнинг хатти-ҳаракатларини кузатиш ва шубҳали фаолиятнинг олдини олиш учун охирги нуқталарни аниқлаш ва уларга жавоб бериш (EDR) ечимларидан фойдаланиш *(EDR - бу охирги қурилмаларда таҳдидларни аниқлаш ва уларга жавоб бериш тизими бўлиб, у Эндпоинт Детестион анд Респонсе синфига мансуб. Бу атама таржимада "охирги қурилмаларда хавфларни аниқлаш ва уларга қарши чора кўриш" маъносини англатади);*

“нол ишонч” (Zero Trust) хавфсизлик тамойилларини қўллаш. Ички ва ташқи ҳар бир кириш сўровини аутентификация қилиш ва текширишни таъминлайдиган нол ишонч тамойилларини жорий этиш;

давлат ва хусусий сектор ўртасида ахборот алмашинувини кучайтириш. Давлат-хусусий шерикликни кенгайтириш орқали таҳдидлар тўғрисида маълумот алмашиш ва товламачи дастурлар

кампанияларига мувофиқлаштирилган жавоб чораларини ишлаб чиқиш учун давлат ва хусусий сектор ўртасидаги ҳамкорликни ривожлантириш;

трансчегаравий ҳамкорлик ва халқаро ташкилотлар билан ўзаро ҳамкорликни ривожлантириш. Товламачилар гуруҳлари фаолиятини тергов қилиш ва уларни жавобгарликка тортишда трансчегаравий ҳамкорликка кўмаклашувчи шартномаларни ишлаб чиқиш. Шу билан биргаликда, Интерпол ва БМТ каби ташкилотлар орқали товламачи дастурларни тарқатиш тармоқларини кузатиш ва йўқ қилиш учун ахборот алмашиш механизмларини кучайтириш.

Хулоса қилиб айтганда, кибертовламачилик жиноятлари ахборотлашган жамият шароитида барқарор ривожланишга жиддий таҳдид солувчи омиллардан бири ҳисобланади. Ушбу жиноят турига қарши курашишда фақат ҳуқуқий чоралар билан чекланиб қолмасдан, ташкилий, техник ва маърифий механизмларни уйғун ҳолда амалга ошириш зарур. Илмий-амалий таҳлиллар шуни кўрсатадики, кибертовламачиликка қарши самарали кураш жамиятнинг киберхавфсизлик маданиятини ошириш билан чамбарчас боғлиқ.