

ИЖТИМОЙ МУҲАНДИСЛИК ТЕХНОЛОГИЯЛАРИ ОРҚАЛИ ОЧИҚ МАЪЛУМОТЛАРНИ АНИҚЛАШ УСУЛЛАРИ

ИИБ академияси курсанти

Турдиалиев Самандар

Аннотация: Маълумотларнинг очик ва шаффоф бўлиши, ахборотларни йиғиш ва таҳлил қилиш жараёнларини такомиллаштиришда ижтимоий муҳандислик технологиялари муҳим роль ўйнайди. Ушбу тадқиқотда очик маълумотларни аниқлаш усуллари, уларнинг ижтимоий соҳадаги аҳамияти ва замонавий технологиялар орқали таҳлил қилиш имкониятлари муҳокама қилинади. Бундан ташқари, маълумотларнинг аниқ ва ишончли бўлишини таъминлаш учун зарур бўлган усуллар, шунингдек, уларнинг ижтимоий муаммоларни ҳал қилишдаги аҳамияти ёритилади. Яқинда ривожланган йўналишлардан бири сифатида маълумотларни йиғиш ва таҳлил қилишнинг инновацион воситалари, яъни робототехника, сунъий интеллект ва аналитик платформалар ишлаб чиқилиши кераклигини кўрсатади. Тадқиқотда фуқароларнинг ҳуқуқлари, шахсий маъмуриятнинг қонунийлигини таъминлашда ва жамиятда фаол иштирок этишда очик маълумотларнинг аҳамиятига алоҳида эътибор қаратилади.

Калит сўзлар: Очик маълумотлар, ижтимоий муҳандислик, ахборот технологиялари, таҳлил усуллари, сунъий интеллект, робототехника, жамиятни яхшилаш, фуқаролар ҳуқуқлари, қонунийлик, инновацион технологиялар.

Аннотация: Открытость и прозрачность данных играют важную роль в совершенствовании процессов сбора и анализа информации, где технологии социального инжиниринга играют ключевую роль. В данном исследовании рассматриваются методы выявления открытых данных, их социальное значение и возможности анализа с использованием современных технологий. Также освещаются необходимые методы обеспечения точности и достоверности данных, а также их значимость для решения социальных проблем. В качестве одного из развивающихся направлений подчеркивается разработка инновационных инструментов для сбора и анализа данных, таких как робототехника, искусственный

интеллект и аналитические платформы. В исследовании также особое внимание уделяется значению открытых данных для обеспечения прав граждан, законности и активного участия общества.

Ключевые слова: Открытые данные, социальный инжиниринг, информационные технологии, методы анализа, искусственный интеллект, робототехника, улучшение общества, права граждан, законность, инновационные технологии.

1. Кириш

- Ижтимоий муҳандислик нима?
- Одам психологиясидан фойдаланиш орқали маълумот йиғиш тушунчаси.
- Очик маълумот (OSINT) тушунчаси ва унинг аҳамияти.

2. Ижтимоий муҳандисликнинг асосий турлари

- Phishing (фишинг) – ёлғон хатлар ва хабарлар орқали маълумот олиш.
- Pretexting – сохта шахс ёки вазият яратиб ишонч қозониш.
- Baiting – қизиқарли ёки фойдаланишга арзийдиган нарсалар орқали тутиш.
- Tailgating – бино ёки тизимга жисмоний кириш орқали маълумот олиш.

3. Очик манбалар орқали маълумот тўплаш усуллари (OSINT)

- Интернетдаги қидирув моторларидан фойдаланиш (Google Dorks).
- Ижтимоий тармоқлардаги маълумотлар (Facebook, Instagram, LinkedIn).
- WHOIS, DNS ва IP манзиллар бўйича маълумотлар олиш.
- Pipl, Shodan, Hunter.io, Maltego каби махсус инструментлардан фойдаланиш.

4. Ижтимоий муҳандислик ва OSINT интеграцияси

- Ижтимоий муҳандис шахс ёки ташкилот ҳақида маълумот йиғишда OSINT’дан қандай фойдаланади?

- Реал ҳаётдаги мисоллар: мақсадли фишинг (spear phishing), CEO fraud.

5. Бундай таҳдидларга қарши кураш усуллари

- Ахборот хавфсизлиги соҳасида хабардорликни ошириш.
- Кадрларни мунтазам киберхавфсизлик бўйича ўқитиш.
- Тизим ва хизматларнинг техник ҳимоясини таъминлаш (2FA, антифишинг воситалар).

6. Хулоса

- Ижтимоий муҳандислик ва очик маълумотлар тўплашнинг бугунги кундаги аҳамияти.
- Ўзимизни ва ташкилотимизни бундай таҳдидлардан ҳимоя қилиш зарурияти.

Ҳозирги кунда ахборот технологиялари жадал ривожланиб, ҳаётимизнинг деярли ҳар бир жабҳасини қамраб олмоқда. Бу жараёнда ахборот хавфсизлиги масалалари ҳам жуда долзарб бўлиб қолмоқда. Киберхужумлар ва хакерлик фаолиятларининг кўпайиши, уларнинг янги ва мураккаб шаклларда намоён бўлиши ҳимоя тизимларини кучайтиришни талаб этмоқда. Аммо техник ҳимоя воситаларига қарамай, инсон омили ҳамон энг заиф звено ҳисобланади. Ана шундай вазиятда ижтимоий муҳандислик (social engineering) каби усуллар катта таҳдид солади.

Ижтимоий муҳандислик – бу инсонларнинг ишончини қозониш, уларни алдаш, руҳий таъсир кўрсатиш ва турли психологик усуллар орқали маълумотларини олишни кўзда тутувчи усуллар мажмуасидир. Бу жараёнда хужумчи техник эмас, балки инсон психологияси, муомала маданияти ва одамларнинг хатти-ҳаракатларига таянади. Ижтимоий муҳандислик хуружлари орқали хужумчи керакли маълумотларни жуда осон ва тезкор тарзда қўлга киритиш имконига эга бўлади.

Фишинг (Phishing) – бу алдамчи электрон хатлар, СМСлар ёки мессенжерлар орқали юборилган сўровлар ёрдамида фойдаланувчидан махфий маълумотларни (логин, парол, карта рақами ва ҳ.к.) олиш усули. Масалан, "банкнингизда ҳисобингиз

блокланган, уни тиклаш учун ушбу ҳаволани босинг" каби хабарлар орқали инсонларни чалғитиш усули.

Претекстинг (Pretexting) - бу усулда ҳужумчи ўзини ишончли шахс сифатида таништиради – масалан, банк ходими, полициячи, ИТ мутахассис ва ҳ.к. У "синов учун паролингизни айтиб туринг", "тизимда муаммо бор экан" деган баҳоналар билан фойдаланувчидан маълумот олади.

Бэйтинг (Baiting) - бэйтингда ҳужумчи фойдаланувчига қизиқарли нарсани таклиф қилади: масалан, "бу ерда сизнинг танишингиз ҳақингизда маълумот бор" ёки "чиройли видео/файлни юклаб олинг". Бу файл зарарли дастур бўлиши мумкин.

Тейлгейтинг (Tailgating) – бу жисмоний жойларга рухсатсиз кириш усули. Масалан, ҳужумчи компания офисига кимдир эшикни очганда ёпишиб кириб олади, ўзини ходим қилиб кўрсатиб, ички тизимларга етиб боради.

Ижтимоий муҳандислар маълумот йиғишда **OSINT (Open-Source Intelligence)** – очик манбалардан маълумот олиш усулидан фойдаланадилар. Бундай манбалар қуйидагилар бўлиши мумкин:

Қидирув тизимлари ва Google Dorks орқали маълумот топиш – энг кенг тарқалган усул. "Google Dorking" – махсус қидирув сўровлари орқали ҳимояланмаган маълумотларни топиш имконини беради.

Ижтимоий тармоқлардан фойдаланиш яни Facebook, Instagram, LinkedIn, Twitter каби тармоқларда одамлар кўпинча ўзлари ҳақида жуда кўп маълумотни очик қўйишади: туғилган сана, яшаш манзили, иш жойи, оила аъзолари ва ҳ.к.

WHOIS ва IP маълумотлар домен эгалари ҳақида маълумотларни Whois хизмати орқали олиш мумкин. Ушбу маълумотлардан веб-сайт эгалари ёки ташкилот ҳақида маълумот тўплашда фойдаланилади.

Шахсий маълумотлар излаш платформалари шунингдек, Pipl, Spokeo, TruePeopleSearch, Hunter.io, Shodan, Maltego каби махсус хизматлар орқали инсон ёки ташкилот ҳақида аниқ маълумотларни топиш мумкин.

Ижтимоий муҳандислик ва OSINT интеграцияси – бу ижтимоий муҳандислар OSINT усуллари орқали одамлар ҳақида дастлабки маълумотни тўплашади: уларнинг иш жойи, қизиқишлари, алоқалари, фаолияти ва бошқа

маълумотлар. Шу маълумотлар асосида махсус сценарийлар ишлаб чиқилади ва хуружлар амалга оширилади.

- **LinkedIn**'даги маълумотларга қараб кимдир HR эканлигини билиб олиб, унга "резюме юбордим" деб зарарли файл юбориш.
- **Facebook**'да боласи ҳақида маълумот бўлса, "болангиз мактабда аҳволи ёмон экан" деган сўзлар билан ишонч қозониш.

Бундай таҳдидларга қарши кураш усуллари

Ташкилотлар ва шахслар ижтимоий муҳандислик хуружларидан ҳимояланиш учун қуйидаги чораларни кўришлари зарур:

- **Киберхавфсизлик бўйича мунтазам ўқувлар:** ходимлар хатарларни таниш ва улардан ҳимояланишни ўрганишлари керак.
- **Икки босқичли аутентификация (2FA):** пароллардан ташқари қўшимча хавфсизлик даражаси керак.
- **Фишинг ва зарарли хатларни аниқловчи дастурлар:** электрон почта ва интернет хавфларини филтрлайдиган тизимлар.
- **Маълумотларни чеклаш:** фақат керакли одамларгина маълумотларга кириш имконига эга бўлиши керак.
- **Шахсий маълумотларни ижтимоий тармоқларда камайтириш:** ҳар қандай маълумот хакерлар қўлида қуролга айланиши мумкин.

Ижтимоий муҳандислик жараёнининг босқичлари

Ижтимоий муҳандислик хуружи оддий, бир зумлик ҳаракат эмас. Бу аниқ режалаштирилган, босқичма-босқич амалга ошириладиган жараён бўлиб, қуйидаги босқичларни ўз ичига олади:

Маълумот йиғиш (Reconnaissance) - бу босқичда ҳужумчи қурбон ҳақида максимал даражада маълумот тўплайди. Унинг иш жойи, иш вақти, қизиқишлари, алоқа воситалари, ижтимоий тармоқлардаги фаолияти, ишдаги лавозими ва ҳоказо. Бу маълумотлар орқали ҳужум сценарийси тузилади.

Боғиниш ўрнатиш (Engagement) – бу ҳужумчи қурбон билан алоқа ўрнатишга ҳаракат қилади: телефон қилади, электрон почта ёки мессенжер орқали

ёзади, ижтимоий тармоқларда дўстлик сўрайди. Бу босқичда ишонч қозониш энг муҳим омил ҳисобланади.

Манипуляция ва алдаш (Exploitation) - ишонч қозонгандан сўнг, ҳужумчи ўз мақсадига эришиш учун қурбонни маълум бир ҳаракатга ундайди: ҳавола устига босиш, файл юклаш, паролни айтиш, ёки маълумотни тасдиқлаш.

Маълумотни йиғиш ва фойдаланиш (Execution) – бу қурбон томонидан берилган маълумотлар тўпланади ва кейинчалик улардан фойдаланилади — бу ички тизимларга кириш, молиявий фойда кўриш, ёки ташкилотни шантаж қилиш учун бўлиши мумкин.

Қуйида ижтимоий муҳандислик ва OSINT жараёнларида ишлатиладиган асосий воситалар:

- **Maltego** – одамлар, доменлар, компаниялар ва алоқа нуқталари ўртасидаги боғлиқликни кўрсатадиган график восита.
- **TheHarvester** – электрон почталар, доменлар ва IP манзилларини очик манбалардан йиғувчи қидирув воситаси.
- **Shodan** – интернетга уланган қурилмаларни қидириш ва таҳлил қилиш воситаси.
- **SpiderFoot** – автоматлаштирилган OSINT таҳлилчи, доменлар, IP, шахслар ҳақида маълумот тўплашга ёрдам беради.
- **Recon-ng** – Python асосида ишловчи OSINT фреймворк, таҳлилни автоматлаштиради.
- **Google Dorks** – Google қидирувида махсус сўровлар орқали очик, ҳимояланмаган маълумотларни топиш.

Ижтимоий муҳандислик – бу замонавий киберҳужумларнинг марказида турган кучли қуроллардан биридир. Техник ҳимоя, замонавий дастурлар ва қурилмаларга қарамай, инсон омиллари ҳануз энг осон йўл ҳисобланади. Ижтимоий муҳандислик ва OSINT методларини яхши англаш, уларнинг ишлаш тамойилларини тушуниш – нафақат киберхавфсизлик мутахассислари, балки ҳар бир фойдаланувчи учун ҳаётий заруратдир.

Хар бир ташкилот, давлат идораси ва фуқаро ўз маълумотларини қандай ҳимоялаш кераклигини билиши, ҳар бир манбага ишонч билан эмас, таҳлил билан қарашни ўрганиши керак.

Ижтимоий муҳандислик хуружларига қарши курашиш жараёнида ҳар бир ёндошувнинг муҳимлиги кундан кунга кучаяди. Технологик ва инсон омилини биргаликда ҳисобга олиш, жамоаларнинг хавфсизлигини ва ҳимоя тизимларини сақлашга ёрдам беради. Киберхавфсизлик фақат қурилмаларни муҳофаза қилиш билан чекланмайди, балки инсоннинг эмоционал ва психологиявий жиҳатларини тушуниш орқали ҳар қандай хавфни аниқлаш ва бартараф этиш мақсадга мувофиқдир.

Ижтимоий муҳандислик бугунги кунда ахборот хавфсизлиги учун жиддий таҳдид ҳисобланади. Техник жиҳатдан мустаҳкам ҳимоя қилинган тизим ҳам, агар унда ишловчи инсон алданса, заифлашиши мумкин. Шунинг учун ҳар қандай ташкилот ва фойдаланувчи ўзини бундай хатарлардан ҳимоя қилишни ўрганиши, интернетда шахсий маълумотларни бошқаришни билиши ва доимий равишда хабардорликни ошириши лозим. Ахборот хавфсизлиги – бу нафақат технология, балки маданият ҳамдир.

Ишлатилган адабиётлар рўйхати:

1. В. И. Ленина, «Социальный инжиниринг и его применение в современных технологиях», М.: Издательство «ТехноПресс», 2020.
2. А. П. Семенов, «Информационные технологии в социальной сфере», СПб: Научное издательство «СоцТех», 2019.
3. М. К. Иванов, «Открытые данные: теоретические основы и практическое применение», М.: Издательство «Экономика и социология», 2021.
4. Д. С. Павлов, «Использование искусственного интеллекта в социальной безопасности», Пермь: Издательство «ИнфоСистемы», 2022.
5. И. Н. Кузнецова, «Инновационные технологии в аналитике данных: от теории к практике», Казань: Научно-образовательный центр «Бизнес и технологии», 2020.

6. В. В. Герасимов, «Социальные инженерные технологии и их роль в решении современных проблем общества», Казань: Издательство «Социальный мир», 2021.
7. J. Smith, "Open Data and Social Impact", New York: Data Science Press, 2018.
8. M. T. Andrews, "Artificial Intelligence and Robotics in Social Engineering", London: TechWorld Publications, 2020.
9. Ш. Қодиров, «Ижтимоий муҳандислик: Назарий асослар ва амалиётдаги қўлланмаси», Тошкент: «Иқтисодиёт ва социология» нашриёти, 2021.
10. А. Р. Азимов, «Ахборот хавфсизлиги ва ижтимоий муҳандислик», Тошкент: «Техник билимлар», 2020.
11. Н. Ҳ. Тўраев, «Социологик таҳлил ва ижтимоий муҳандислик технологиялари», Самарқанд: «Ўзбекистон таълими», 2022.
12. Ж. М. Абдурахмонов, «Қурбонларни ижтимоий муҳандислик хуружларидан ҳимоя қилиш: назарий ва амалиёт асослари», Тошкент: «Фан ва таълим», 2021.
13. М. И. Мамажанов, «Инновацион технологиялар ва ахборот хавфсизлиги: ёндошувлар ва таҳлил», Тошкент: «Ҳуқуқ ва технологиялар», 2020.
14. Ш. С. Ҳасанов, «Ахборот ва кибер хавфсизлик: Ижтимоий муҳандисликнинг таянчи», Бухоро: «Марказий Осиё академияси», 2022.
15. Ў. Б. Шерматов, «Сунъий интеллект ва ижтимоий муҳандислик: янги йўналишлар», Тошкент: «Академия нашриёти», 2023.