EOC
EUROASIAN ONLINE CONFERENCES

GERMANY
CONFERENCE

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY



Google Scholar zenodo OpenAIRE doi digital object identifier

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY: a collection scientific works of the International scientific conference – Gamburg, Germany, 2025 Issue 5

Languages of publication: Uzbek**,** English, Russian, German, Italian, Spanish,

The collection consists of scientific research of scientists, graduate students and students who took part in the International Scientific online conference **« INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY ».** Which took place in Gamburg, 2025.

Conference proceedings are recommended for scientists and teachers in higher education establishments. They can be used in education, including the process of post - graduate teaching, preparation for obtain bachelors' and masters' degrees. The review of all articles was accomplished by experts, materials are according to authors copyright. The authors are responsible for content, researches results and errors.

Loyiha boshqaruvida kiberxavfsizlik integratsiyasi: Amaliy tajribalar, cheklovlar va signal-tasvir loyihalaridagi qo‘llanilishi

Dalibekov L. R
Katta o’qituvchi Farg‘ona davlat texnika universiteti
Mamatvaliyev D. X
Muhammadaliyev A. A
bakalavr Farg‘ona davlat texnika universiteti

ANNOTATSIYA: Loyiha boshqaruvida raqamli vositalar signal, tasvir va IoT ma’lumotlari bilan real vaqt ishlashi sababli kiberxavfsizlik tahdidlarini oshirmoqda. Tadqiqot Arksey va O’Malley yondashuvi asosida IEEE Xplore, Scopus va Web of Science bazalaridagi adabiyotlarni tahlil qilib, signal va tasvirlarni qayta ishlash bosqichida yuzaga keladigan maxsus xavflarni o‘rgandi. Natijalar shuni ko‘rsatadiki, loyiha menejerlarida ushbu ma’lumotlarni shifrlash, uzatish kanallarini himoyalash va risklarni kamaytirish bo‘yicha yetarli malaka yetishmaydi. Adabiyotlarda amaliy tadqiqotlar va kiberxavfsizlikni loyihaning butun hayot aylanishiga integratsiya qilish bo‘yicha aniq metodik asoslar yetarli emas. Tadqiqot menejerlar uchun amaliy ko‘rsatmalar va sohaga xos xavfsizlik metodologiyalarini ishlab chiqish zarurligini ta’kidlaydi.

ABSTRACT: In project management, extensive use of digital tools that operate in real time with signal, image, and IoT data increases cybersecurity threats. This study explored specific risks that emerge during signal and image processing by analyzing literature from IEEE Xplore, Scopus, and Web of Science using the Arksey and O’Malley approach. The results show that project managers often lack sufficient skills to encrypt this data, secure transmission channels, and mitigate related risks. The literature lacks practical case studies and clear methodological frameworks for integrating cybersecurity throughout the project lifecycle. The study highlights the need to develop practical guidelines and domain-specific security methodologies for project managers.

АННОТАЦИЯ: В управлении проектами активное использование цифровых инструментов, работающих в реальном времени с сигнальными, визуальными и IoT-данными, усиливает угрозы кибербезопасности. В исследовании были изучены специфические риски, возникающие на этапе обработки сигналов и изображений, на основе анализа литературы из баз данных IEEE Xplore, Scopus и Web of Science с применением подхода Аркси и О’Малли. Результаты показывают, что проектным менеджерам часто не хватает навыков для шифрования таких данных, защиты каналов передачи и снижения

сопутствующих рисков. В литературе недостаточно практических кейсов и чётких методологических основ для интеграции кибербезопасности на всех этапах жизненного цикла проекта. Исследование подчёркивает необходимость разработки практических рекомендаций и отраслевых методологий киберзащиты для проектных менеджеров.

KALIT SO'ZLAR: kiberxavfsizlik; tashkiliy madaniyat; loyihaning hayot aylanishi; loyihalar boshqaruvi; risklarni boshqarish; kichik va o'rta korxonalar (KO'K); signalni qayta ishlash; tasvirlarni qayta ishlash; kompyuter ko'rish; sensor texnologiyalari; biometrik tasvirlar xavfsizligi; ma'lumotlarni shifrlash; real vaqt signallari; IoT signal xavfsizligi; videoanalitika.

KEYWORDS: cybersecurity; organizational culture; project lifecycle; project management; risk management; small and medium enterprises (SMEs); signal processing; image processing; computer vision; sensor technologies; biometric image security; data encryption; real-time signals; IoT signal security; video analytics.

КЛЮЧЕВЫЕ СЛОВА: кибербезопасность; организационная культура; жизненный цикл проекта; управление проектами; управление рисками; малые и средние предприятия (МСП); обработка сигналов; обработка изображений; компьютерное зрение; сенсорные технологии; безопасность биометрических изображений; шифрование данных; сигналы в реальном времени; безопасность IoT-сигналов; видеоаналитика.

KIRISH. Kiberxavfsizlikni loyiha boshqaruviga integratsiyalash texnologik muhitlarning murakkabligi va kiber tahdidlarning kuchayishiga javoban muhim e'tibor sohasi sifatida paydo bo'ldi. Loyihani amalga oshirishda raqamli infratuzilmalarga tobora ortib borayotgan bog'liqlik, ayniqsa signal va tasvirlarni qayta ishlashga asoslangan tizimlardan (sensor tarmoqlari, videoanalitika, biometrik identifikatsiya, IoT qurilmalaridan keladigan real vaqt signallari) foydalanilayotgan sharoitda, loyiha boshlanganidan boshlab kiberxavfsizlikni hisobga olishni talab qiladi. Tashkilotlar loyiha vaqt jadvallari va byudjetlarini saqlab qolish bilan birga nozik ma'lumotlarni, jumladan raqamli signallar va tasvirlarda aks etgan maxfiy axborotni himoya qilish muammosiga duch kelmoqdalar. Bu esa kiberxavfsizlikning ushbu jarayonlarga integratsiyasidagi ilg'or tajribalar va mavjud bo'shliqlarni o'rganadigan adabiyotlarning tobora ko'payishiga olib kelmoqda.

Loyihani boshqarish instituti (PMI) loyihani muvaffaqiyatli boshqarishning asosiy komponenti sifatida risklarni, shu jumladan kiberxavfsizlik risklarini boshqarish muhimligini ta'kidlaydi. Tadqiqotlar

shuni ko‘rsatadiki, ko‘plab loyiha menejerlarida kiberxavfsizlik xavfini samarali hal qilish uchun zarur treninglar va vositalar yetishmaydi. Bu, ayniqsa, signal va tasvirlarni qayta ishlashda uchraydigan maxsus tahdidlar — tasvirlarni soxtalashtirish (deepfake), signalga zararli paketlar qo‘shilishi, aqlli sensorlar orqali tajovuzlar, tarmoq orqali uzatilayotgan tasvir/signal oqimlarining o‘g‘irlanishi yoki o‘zgartirilishi — kabi zaifliklarga olib kelishi mumkin.

Loyihaning murakkabligi oshgani sayin, an’anaviy loyihalarni boshqarish tizimlari ko‘pincha kiberxavfsizlikni, xususan signal va tasvirlarni qayta ishlash jarayonlaridagi himoya mexanizmlarini hisobga olmaydi. Bu esa tashkilotlar uchun jiddiy oqibatlarga olib kelishi mumkin, chunki tasvirga asoslangan monitoring tizimlaridagi buzilishlar, signalni qayta ishlashdagi xatoliklar yoki raqamli video ma’lumotlarning himoyasizligi operatsion falokatlarga sabab bo‘lishi mumkin. Shu sababli joriy amaliyotlarni aniqlash va qo‘shimcha tadqiqotlar va ishlanmalar zarur bo‘lgan muhim kamchiliklarni belgilash uchun tizimli, qamrovli tekshiruv talab etiladi.

Bundan tashqari, kiberxavfsizlikni loyiha boshqaruviga integratsiya qilish nafaqat texnik choralarni, balki tashkilot madaniyati va manfaatdor tomonlarning ishtirokini ham o‘z ichiga oladi. Tashkilotlar loyihaning barcha manfaatdor tomonlarida, ayniqsa signal va tasvirlar bilan ishlaydigan texnik jamoalarda, kiberxavfsizlikdan xabardorlikni birinchi o‘ringa qo‘yadigan madaniyatni rivojlantirishlari kerak. Chunki inson omillari ko‘pincha signal ma’lumotlarining noto‘g‘ri qayta ishlanishi, ruxsatsiz kirish yoki tasvirlar bilan ishlashdagi beparvolik sababli eng zaif bo‘g‘in hisoblanadi. Agile va Waterfall metodologiyalari kabi loyihalarni boshqarishning mavjud asoslari kiberxavfsizlik tamoyillarini samarali kiritish uchun moslashishni talab qiladi. Bu jarayon signal va tasvirlarni qayta ishlashning barcha bosqichlarida — yig‘ish, filtrlash, tahlil qilish, saqlash, uzatish va vizualizatsiya qilishda — xavfsizlikni ko‘zda tutadigan moslashtirilgan yondashuv zarurligini bildiradi.

Bu loyiha boshqaruvi va kiberxavfsizlik landshaftlarining rivojlanayotgan tabiatini aks ettiruvchi, xususan signal va tasvirlarni qayta ishlashga xos tahdidlarga javob beradigan integratsiyalashgan metodologiyalarni ishlab chiqish bo‘yicha doimiy izlanishlar zarurligini ta’kidlaydi. Kiberxavfsizlikni loyihalarni boshqarishga integratsiyalashuvi tobora muhim ahamiyat kasb etmoqda, chunki tashkilotlar loyiha muvaffaqiyatini xavf ostiga qo‘yadigan ko‘plab kibertahdidlarga duch kelmoqda. Maxfiy informatsiyani, shu jumladan tasvirlar, audio signallar, sensor ma’lumotlari va video oqimlarini himoya qilish hamda operatsion yaxlitlikni saqlash muhimligining oshishiga qaramay, ko‘plab loyihalarni boshqarish tizimlari kiberxavfsizlik xavfini yetarli darajada hal qila olmaydi.

Mavjud tadqiqotlar loyiha boshqaruvi, kiberxavfsizlik va signal/tasvirlarni qayta ishlash amaliyotlari o‘rtasidagi sezilarli uzilishni ta’kidlaydi.

Bundan tashqari, loyiha menejerlari ko‘pincha kiberxavfsizlik tahdidlarini samarali aniqlash va yumshatish uchun zarur tayyorgarlik va resurslarga ega emas, bu esa risklarni boshqarishga proaktiv emas, balki reaktiv yondashuvni keltirib chiqaradi. Bu holat ayniqsa signal va tasvirlarni qayta ishlash texnologiyalaridan foydalaniladigan loyihalarda sezilarli bo‘lib, real vaqt ma’lumotlar oqimidagi buzilishlar, tasvirlarni soxtalashtirish, sensor signallariga zararli paketlarning qo‘shilishi yoki video oqimlarning o‘g‘irlanishi kabi o‘ziga xos tahdidlar reaktiv yondashuvni yanada xavfli qiladi. Bunday tayyorgarlikning etishmasligi kiber hodisalarning ta’sirini kuchaytirishi mumkin, bu esa loyihaning butun hayoti davomida kiberxavfsizlikni hisobga olgan holda, xususan signal va tasvir ma’lumotlarini qayta ishlash bosqichlarida, moslashtirilgan strategiyalarni ishlab chiqish muhimligini ta’kidlaydi. Mavjud adabiyotlar shuni ko‘rsatadiki, tashkilotlar har qanday kiberxavfsizlik strategiyasining samaradorligini aniqlashda muhim bo‘lgan inson omillarini, masalan, tasvirlarni noto‘g‘ri etiketlash, sensor qurilmalarni beparvo sozlash yoki signal oqimlari bilan ishlashda e’tiborsizlik kabi holatlarni ko‘pincha e’tiborsiz qoldiradilar.

Shu sababli joriy amaliyotlarni tizimli ravishda baholash, bilim va joriy etishdagi kamchiliklarni aniqlash va kiberxavfsizlik integratsiyasi bo‘yicha amaliy tavsiyalar berish uchun qamrovli tekshiruvga ehtiyoj bor. Ushbu tadqiqot kiberxavfsizlik va loyihalarni boshqarishning kesishishi bo‘yicha mavjud adabiyotlarni sintez qiluvchi ko‘lamli tekshiruv o‘tkazish orqali ushbu bo‘shliqlarni to‘ldirishga qaratilgan. Mavjud amaliyotlarni aniqlash va qo‘shimcha tadqiqotlarni talab qiladigan sohalarni aniqlash orqali tadqiqot loyiha menejerlari signal va tasvir ma’lumotlariga asoslangan raqamli infratuzilmalarda kiber tahdidlarga chidamlilikni oshirish uchun foydalanishi mumkin bo‘lgan mustahkam asosni ishlab chiqishga yordam beradi. Oxir-oqibat, ushbu tadqiqot ilg‘or tajribalarni shakllantirishga va loyiha boshqaruvi doirasida kiberxavfsizlikdan xabardorlik madaniyatini oshirishga, shu orqali xavflarni kamaytirishga va loyihaning umumiy natijalarini yaxshilashga qaratilgan.

Kiberxavfsizlikni loyiha boshqaruviga integratsiyalash dolzarb muammoga aylandi, chunki tashkilotlar kibertahdidlarning kuchayishi bilan tavsiflangan tobora murakkab raqamli landshaftga duch kelmoqda. Bu murakkablik signal va tasvirlarni qayta ishlash bilan bog‘liq tizimlar — masalan, video kuzatuv, aqlli sensorlar, kompyuter ko‘rish, biometrik tanib olish tizimlari — keng qo‘llanayotgan sektorlarda yanada yaqqol seziladi. Mazkur sohalarda kiberxavfsizlikning buzilishi katta moliyaviy yo‘qotishlarga, obro‘ga putur yetishiga, tasvir yoki signal ma’lumotlarining yo‘qolishi yoki

manipulyatsiyasiga, shuningdek operatsion uzilishlarga olib kelishi mumkin. Bu loyiha menejerlariga kiberxavfsizlikni, jumladan signal va tasvirlarga oid ma'lumotlar xavfsizligini, loyiha jarayonlariga integratsiya qilish zarurligini yana bir bor ta'kidlaydi. Bu bo'shliq loyihalarni boshqarish metodologiyalarini kiberxavfsizlik muammolarini hal qilish uchun qayta ko'rib chiqishni talab qiladi.

Kiberxavfsizlikni loyiha boshqaruviga integratsiyalashning nazariy asosi tizimlar nazariyasi va xavflarni boshqarish bo'yicha o'rnatilgan yondashuvlarga asoslanadi. Tizimlar nazariyasi tashkilot ichidagi turli komponentlarning, jumladan signal yig'ish qurilmalari, ma'lumot uzatish kanallari va tasvirlarni qayta ishlash modullarining o'zaro bog'liqligini ta'kidlaydi. Bu loyihaning samarali boshqaruvi umumiy loyiha ekotizimining ajralmas qismi sifatida signal va tasvirlar bilan ishlaydigan kiberxavfsizlik muhitini hisobga olishi kerakligini ko'rsatadi. Risk Management Frameworks esa xavflarni, shu jumladan signal va tasvirga oid kiber tahdidlarni aniqlash, baholash va yumshatish uchun tizimli yondashuvlarni taklif etadi, bu esa loyiha menejerlariga kiberxavfsizlikni risklarni boshqarish jarayonlariga qo'shishda yordam beradi.

Kiberxavfsizlik integratsiyasiga bo'lgan ehtiyoj ortib borayotganiga qaramay, jiddiy to'siqlar saqlanib qolmoqda. Loyiha menejerlari o'rtasida kiberxavfsizlik, ayniqsa signal va tasvirlar bilan ishlashga oid maxsus xatarlarga doir trening va xabardorlikning yetishmasligi muhim muammo sanaladi. Ko'pgina menejerlar real vaqt video oqimlarida anomaliyalarni aniqlash, tasvirlarni shifrlash, sensor tarmoqlarini himoya qilish yoki tasvir/signalga asoslangan tizimlarga qaratilgan kiber hujumlarni baholash bo'yicha zarur ko'nikmalarga ega emas. Bu esa ko'pincha proaktiv emas, balki reaktiv strategiyalarni yuzaga keltiradi. Tegishli o'quv dasturlarining yo'qligi bu bilimlar bo'shlig'ini yanada chuqurlashtiradi va tashkilotlarning loyiha menejerlarini zarur kiberxavfsizlik kompetensiyalari bilan ta'minlash uchun keng qamrovli ta'lim tashabbuslariga sarmoya kiritish zarurligini ko'rsatadi.

Tashkiliy madaniyat ham kiberxavfsizlikning muvaffaqiyatli integratsiyasida hal qiluvchi rol o'ynaydi. Tadqiqotlar shuni ko'rsatadiki, kiberxavfsizlikdan xabardorlikni birinchi o'ringa qo'yadigan madaniyatni rivojlantirish loyiha guruhlariga signal va tasvirlarni qayta ishlash jarayonlarida yanada mustahkamroq xavfsizlik choralarini qo'llash imkonini beradi. Bunday madaniyat xavfsizlik protokollariga rioya qilishni mustahkamlaydi va xavflarni boshqarishga nisbatan faolroq yondashuvni shakllantiradi. Inson omillari, masalan tasvirlarni noto'g'ri etiketlash, operatorning signalni noto'g'ri talqin qilishi yoki tizim sozlamalaridagi beparvolik kabi xatolar xavfsizlik buzilishlarining asosiy sababi bo'lib qolmoqda. Shu bois inson–kompyuter o'zaro ta'siri (HCI) istiqboli loyiha

jamoalari kiberxavfsizlik vositalari bilan qanday ishlashini yaxshiroq tushunishga yordam beradi, bu esa vositalarning foydalanuvchiga qulay va samarali bo‘lishini ta’minlaydi.

Kiberxavfsizlikni loyiha boshqaruviga integratsiyalashuvi manfaatdor tomonlarning ishtiroki va aloqalarini ham sezilarli darajada kuchaytiradi. Manfaatdor tomonlarni kiberxavfsizlik masalalariga jalb qilish orqali loyiha menejerlari xavfsizlik maqsadlarini loyiha maqsadlari bilan moslashtira oladi, bu esa kiberxavfsizlik choralarining to‘siq emas, balki qo‘llab-quvvatlovchi omilga aylanishiga yordam beradi. Manfaatdor tomonlar nazariyasi ushbu integratsiya jarayonida turli manfaat va pozitsiyalarni hisobga olish zarurligini ta’kidlaydi; samarali muloqot esa jamoalar o‘rtasida hamkorlik va tushunishni kuchaytiradi.

Empirik tadqiqotlar shuni ko‘rsatadiki, kiberxavfsizlikni loyihalarni boshqarish amaliyotiga muvaffaqiyatli integratsiya qilgan tashkilotlar, xususan signal va tasvir mahsulotlariga tayangan tizimlarda, loyiha natijalarining yaxshilanishi va kiber tahdidlarga qarshi yanada chidamli bo‘lib borayotganini ta’kidlaydi. Bu integratsiya risklarni boshqarishga yaxlit yondashuvni shakllantiradi, unda kiberxavfsizlik loyihaning boshlanishidan to yakunigacha bo‘lgan barcha bosqichlarda o‘rnatiladi. Bu nafaqat nozik ma’lumotlarni himoya qiladi, balki signal va tasvirlarni qayta ishlash jarayonlarining ishonchliligini oshiradi va loyihaning umumiy barqarorligini ta’minlaydi.

Shu bilan birga, adabiyotlar ushbu integratsiya bo‘yicha ko‘plab kamchiliklarni ham ko‘rsatadi. Masalan, Agile, Waterfall va gibrid metodologiyalarda kiberxavfsizlik tamoyillarini amaliy qo‘llash bo‘yicha signal va tasvirlarga xos yo‘riqnomalar yetarli emas. Bundan tashqari, tashkilot madaniyati va muvaffaqiyatli integratsiya o‘rtasidagi bog‘liqlik hali to‘liq o‘rganilmagan. Xususan, madaniy omillarning signal va tasvirlarni qayta ishlash tizimlarida kiberxavfsizlik amaliyotlarining samaradorligiga qanday ta’sir qilishi bo‘yicha ko‘proq empirik tadqiqotlar talab etiladi. Kiberxavfsizlik integratsiyasi ahamiyat kasb etayotgan bir paytda, amaliyotda va tushunishda hali ham sezilarli bo‘shliqlar mavjud bo‘lib qolmoqda.

TADQIQOT USULLARI

Ushbu ko‘lamli ko‘rib chiqish Arksey va O'Malley (2005) tomonidan ishlab chiqilgan asosdan so‘ng amalga oshirildi, bu tadqiqot sohasidagi asosiy tushunchalarni xaritalash, adabiyotdagi kamchiliklarni aniqlash va mavjud bilimlarni umumlashtirish uchun tizimli yondashuvni ta’minlaydi. Ushbu ramka o‘zining moslashuvchanligi va kiberxavfsizlik hamda loyihalarni boshqarish kabi keng mavzularni o‘rganish uchun mosligi sababli tanlandi.

Ko‘rib chiqish beshta asosiy bosqichdan iborat bo‘ldi: tadqiqot savolini aniqlash, tegishli tadqiqotlarni aniqlash, tadqiqotlarni tanlash, ma’lumotlarni

jadvalga tushirish va natijalarni umumlashtirish. Jarayon davomida adabiyotlarni aniqlash, tanlash va tahlil qilishda shaffoflik va qat'iylik ta'minlandi. Tadqiqot 2010–2023 yillar oralig'ida chop etilgan, kiberxavfsizlik, loyiha boshqaruvi va ular bilan bog'liq raqamli texnologiyalar, jumladan signal va tasvirlarni qayta ishlash tizimlarini qamrab olgan adabiyotlar bilan cheklangan.

Agar tadqiqotlar ushbu yo'nalishlarning kesishuvini yoritmasa yoki ingliz tilida bo'lmasa, ular chiqarib tashlandi. Bundan tashqari, faqat texnik signalni qayta ishlash masalalariga bag'ishlangan, ammo loyiha boshqaruvi bilan bog'lanmagan maqolalar ham chiqarib tashlandi.

Qidiruv IEEE Xplore, Scopus, Web of Science va Google Scholar bazalarida amalga oshirildi. Qidiruvda "kiberxavfsizlik", "loyiha boshqaruvi", "signal processing", "image processing", "sensor data security", "risk management" kabi kalit so'zlar mantiqiy operatorlar bilan birlashtirildi.

Tanlangan maqolalardan ma'lumotlar standartlashtirilgan shakl asosida chiqarib olindi: tadqiqot maqsadi, metodologiyasi, asosiy topilmalari, qo'llanilgan **signal/tasvirni qayta ishlash yondashuvlari** (masalan, real vaqt monitoringi, anomaliyani aniqlash algoritmlari, biometrik autentifikatsiya), va loyiha boshqaruvi uchun amaliy ta'sirlari qayd etildi.

NATIJALAR

Qidiruvlar natijasida jami **642 ta tadqiqot** aniqlandi. 123 ta dublikat olib tashlangach, 519 ta maqolaning sarlavha va annotatsiyalari tahlil qilindi. Ulardan 311 tasi mavzuga mos kelmagani uchun chiqarildi. Qolgan 208 ta to'liq matn ko'rib chiqilib, 144 tasi mezonlarga mos kelmagani sababli chiqarib tashlandi. Yakuniy sharhga 64 ta maqola kiritildi.

Bu tadqiqotlarning bir qismi signalga oid yondashuvlarni o'z ichiga oladi, xususan:

real vaqtli sensor signallari orqali xavfsizlik buzilishlarini aniqlash,
video tasvirlar yordamida obyektlar va anomal faoliyatni kuzatish,
biometrik tasvirlar (yuz, barmoq izi) orqali foydalanuvchi autentifikatsiyasi,
signal asosidagi kiberhujumlarni (masalan, IoT qurilmalardagi elektromagnit shovqin) monitoring qilish.

Bu texnologiyalar kiberxavfsizlikni loyiha boshqaruvi jarayonlariga integratsiya qilishda tobora keng qo'llanayotganini ko'rsatadi.

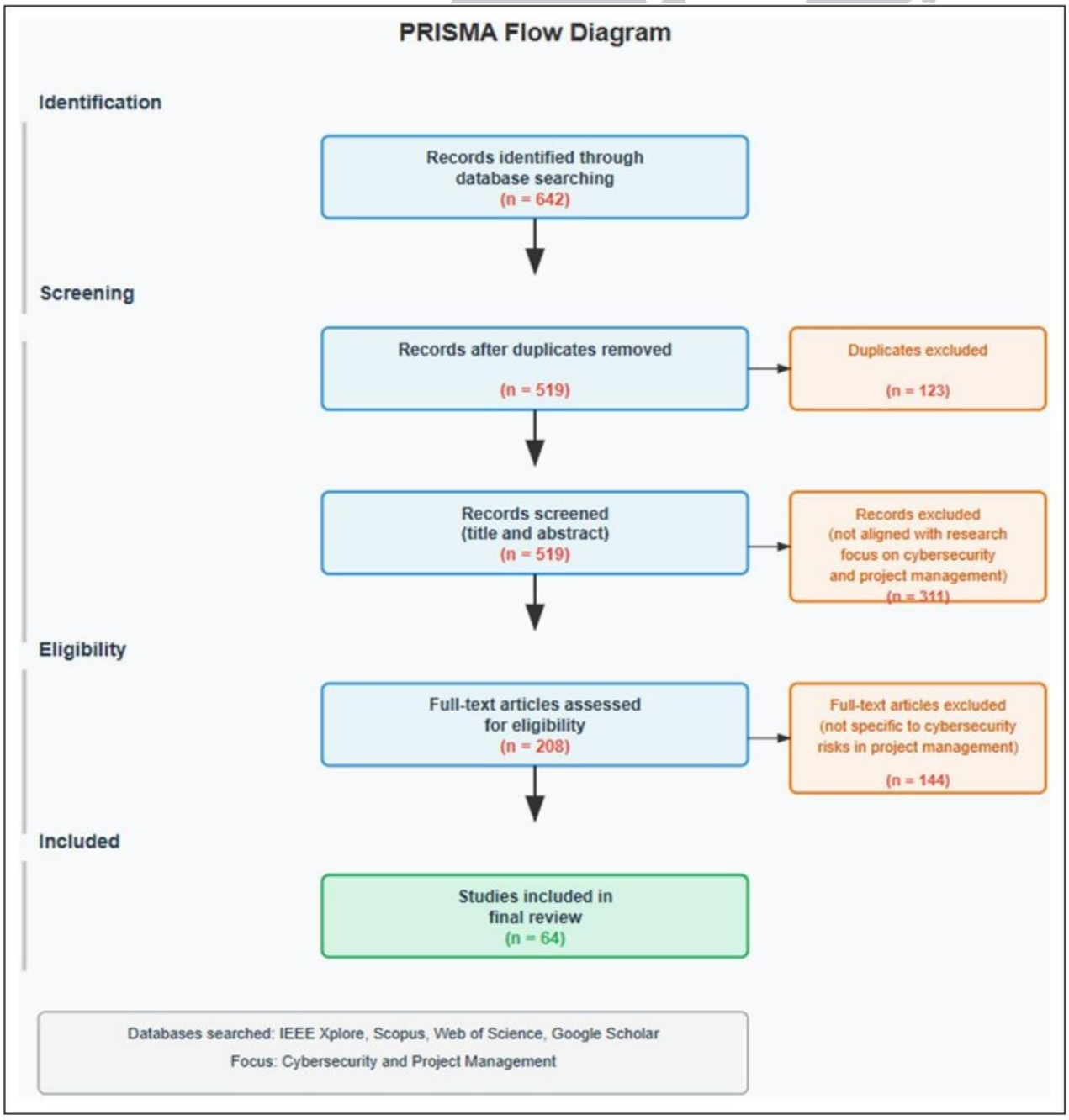
KIRITILGAN TADQIQOTLARNING XUSUSIYATLARI

Ko'rib chiqilgan 64 ta tadqiqot quyidagilarni o'z ichiga oldi:

tasvirni qayta ishlash asosidagi xavfsizlik monitoringi tizimlari,
sensor ma'lumotlardan foydalangan holda anomaliyani aniqlash algoritmlari,
IoT qurilmalarida signal xavfsizligi,
videoanalitika orqali xavflarni erta aniqlash,

real vaqt signallarini qayta ishlash orqali loyiha jarayonlarida riskni monitoring qilish.

Bu esa shuni ko‘rsatadiki, kiberxavfsizlik va loyiha boshqaruvi kesishmasi endilikda faqat tashkiliy va strategik boshqaruv bilan cheklanmay, balki signal va tasvirlarni qayta ishlash kabi texnik intellektual yondashuvlarni ham o‘z ichiga oladi.



Ular orasida 45% tadqiqotlarda amaliy tadqiqotlar va intervyular kabi sifatli tadqiqot dizaynlaridan foydalanilgan, 35% so‘rovlar va statistik tahlillarni o‘z ichiga olgan miqdoriy yondashuvlarga asoslangan. Qolgan 20%

tadqiqotlarda masalalarni kengroq tekshirish uchun aralash usullar qo‘llangan. Ko‘pgina tadqiqotlar (85%) yirik korxonalarga qaratilgan bo‘lib, tanlov hajmi 50 dan 500 dan ortiq ishtirokchilarni tashkil etgan, atigi 15% kichik va o‘rta korxonalarni (KO‘B) o‘rganib chiqqan. Bu adabiyotda sezilarli bo‘shliqni ko‘rsatadi, chunki KO‘B cheklangan resurslar tufayli signal va tasvirlarni qayta ishlash tizimlarida kiberxavflarga nisbatan sezgir bo‘lishi mumkin. Tadqiqotlar asosan rivojlangan mamlakatlarda (70%) olib borilgan, rivojlanayotgan mamlakatlar faqat 30% ni tashkil qilgan, bu esa topilmalarning kam resurslarga ega bo‘lgan kontekstlarga umumlashtirilishi haqida savollarni tug‘diradi. Nashr qilingan yillar 2010 yildan 2023 yilgacha bo‘lib, so‘nggi besh yil ichida kiberxavfsizlikning signal va tasvirlarni qayta ishlash loyihalaridagi ahamiyati ortib borayotganini aks ettiradi. Tadqiqotlarning asosiy diqqat markazi turlicha bo‘lib, 50% xavflarni boshqarish amaliyotiga, 30% kiberxavfsizlikdan xabardorlik va loyiha menejerlari uchun treningga, 20% esa texnologik aralashuvlarga qaratilgan.

Tematik jihatdan, ko‘rib chiqish natijalari signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlikning integratsiyasi bo‘yicha muhim fikrlarni ochib berdi. Tadqiqotlar davomida asosiy mavzu kiberxavfsizlikning asosiy loyiha xavfi sifatida tobora e’tirof etilishi bo‘lgan, ayniqsa raqamli transformatsiya yoki signal va tasvirlarni qayta ishlash texnologiyalaridan foydalanishni o‘z ichiga olgan loyihalarda. Tadqiqotchilarning ta’kidlashicha, loyiha menejerlari ko‘pincha kiberxavfsizlik bo‘yicha etarli bilimga ega emas, bu esa signal va tasvirlarni qayta ishlash tizimlarini kiberhujumlarga qarshi himoyasiz qoldiradi. Bir nechta tadqiqotlarda kiberxavfsizlikni moliyaviy yoki operatsion risklarga o‘xshash tarzda loyiha hayoti davomida risklarni boshqarish jarayonlariga kiritish zaruriyati ta’kidlangan.

Yana bir muhim topilma loyiha boshqaruviga kiberxavfsizlikni integratsiyalash bo‘yicha ilg‘or tajribalarni aniqlash bo‘ldi. Ko‘plab tadqiqotlar loyihani boshlash paytida kiberxavfsizlik bo‘yicha mutaxassislar bilan erta hamkorlik qilish, potentsial kibertahdidlarni doimiy monitoring qilish va favqulodda vaziyatlar rejalarini ishlab chiqishni tavsiya qilgan. Loyihalar guruhlari proaktiv yondashuvni qo‘llashi kerak. Ko‘pgina tadqiqotlar, shuningdek, signal va tasvirlarni qayta ishlash loyihalarida xavflarni yumshatishda texnologiyaning rolini ta’kidladi. Masalan, ilg‘or shifrlash texnologiyalari va ko‘p faktorli autentifikatsiyani o‘z ichiga olgan xavfsiz tizimlarni joriy qilish tavsiya qilingan, biroq cheklangan resurslarga ega bo‘lgan kichik tashkilotlar uchun ushbu tadbirlarni amalga oshirish qiyin bo‘lishi mumkin. Bundan tashqari, Crespo va Taboada (2021) hamda Xarrington (2020) loyihani amalga oshirish jarayonida javob tezligi va aniqligini oshirish uchun kiberxavfsizlik tahdidlarini aniqlashni avtomatlashtirish muhimligini ta’kidlagan.

Signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlikdan xabardorlik va tashkiliy madaniyat ham katta ahamiyatga ega. Ghandour (2019) va Williams va Hardy (2017) tadqiqotlari ko‘rsatdiki, kiberxavfsizlik umumiy mas’uliyat sifatida qaraladigan kuchli xavfsizlik madaniyatiga ega bo‘lgan tashkilotlar loyihalarida kiber hodisalar soni pastroq bo‘ladi. Ushbu tadqiqotlar salohiyatni oshirish tashabbusining bir qismi sifatida loyiha menejerlari va jamoalari uchun kiberxavfsizlikdan xabardorlik dasturlarini kiritishni targ‘ib qiladi. Alotaybi shuningdek, kiberxavfsizlik xatarlari bo‘yicha ochiq muloqotni qo‘llab-quvvatlagan tashkilotlar kibertahdidlarni samarali tarzda yumshatish imkoniga ega ekanligini ko‘rsatdi.

Tadqiqotlar soni ortib borayotganiga qaramay, adabiyotda bir nechta bo‘shliqlar mavjud. Birinchidan, KO‘Bning signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlikni integratsiyalash bo‘yicha empirik tadqiqotlar sezilarli darajada yetishmaydi, garchi bu korxonalar cheklangan resurslar tufayli kiberhujumlarga nisbatan sezgir bo‘lsa ham. Bundan tashqari, sog‘liqni saqlash, qurilish va ta’lim kabi tarmoqlarda signal va tasvirlarni qayta ishlashga oid kiberxavfsizlik tadqiqotlari yetarlicha o‘rganilmagan. Shuningdek, kiberxavfsizlik strategiyalarining uzoq muddatli samaradorligini baholovchi uzunlamas tadqiqotlar yo‘q. Ko‘plab tadqiqotlar eng yaxshi amaliyot va strategiyalarni ta’kidlagan bo‘lsa-da, bir nechtasi loyiha menejerlariga turli loyiha turlari va sektorlarida amalga oshirish mumkin bo‘lgan amaliy, sanoatga xos asoslarni taklif qiladi. Nihoyat, rivojlanayotgan mamlakatlarda raqamli infratuzilma va tartibga solish muhiti rivojlangan mintaqalardan farq qilishi mumkin, bu esa loyiha menejerlari uchun signal va tasvirlarni qayta ishlash tizimlarida kiberxavfsizlik choralarini kontekstga mos integratsiyalash bo‘yicha qo‘shimcha tadqiqotlar zarurligini ko‘rsatadi.

Ko‘lamli tahlil natijalari shuni ko‘rsatadiki, kiberxavfsizlik signal va tasvirlarni qayta ishlash loyihalarida tobora muhim tarkibiy qismga aylangan, loyihalarni rejalashtirish, amalga oshirish va monitoring qilishga sezilarli ta’sir ko‘rsatadi. Loyihalarni boshqarish tizimlariga kiberhujumlarning tobora ko‘payib borayotgani kiberxavfsizlikni xavflarni boshqarish jarayonining ajralmas qismiga aylantiradi. Tadqiqotlar loyiha menejerlarida ko‘pincha kiberxavfsizlik bo‘yicha zarur bilimlarning yetishmasligini ko‘rsatdi, bu esa loyihalarni sezilarli zaifliklarga olib keladi. Ekspertizadagi bu bo‘shliq loyiha menejerlari uchun signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlik tamoyillari bo‘yicha maxsus treninglar zarurligini ko‘rsatadi. Bu esa shuni anglatadiki, loyihaning muvaffaqiyatini ta’minlash uchun, ayniqsa raqamli platformalar va algoritmlarga juda bog‘liq sohalarda, loyiha guruhlari loyiha boshlanganidan boshlab va uning butun hayoti davomida kiberxavfsizlikni birinchi o‘ringa qo‘yishlari kerak.

Shuningdek, ushbu sharhda kiberxavfsizlik bo‘yicha mutaxassislar bilan erta hamkorlik qilish, muntazam auditlar va xavfsiz signal va tasvirlarni qayta ishlash vositalarini joriy etish kabi ilg‘or tajribalarni qo‘llash muhimligi ta’kidlangan. Bu strategiyalar nafaqat kiberxavflarni yumshatadi, balki manfaatdor tomonlarning ishonchini oshiradi, chunki ular loyihalardagi ma’lumotlar va jarayonlarning xavfsizligi haqida tobora ko‘proq tashvishlanmoqda. Ushbu choralarni o‘z ichiga olgan loyihalar, xususan, IT va moliya kabi raqamli operatsiyalar uchun muhim bo‘lgan sohalarda muvaffaqiyatli natijalarga erishish ehtimoli yuqori. Shu sababli, loyiha menejerlari hozirgi texnologik landshaftda kibertahdidlarga ta’sir kuchayganini tan olgan holda, kiberxavfsizlik strategiyalarini joriy etish uchun o‘z rollarini rivojlantirishlari lozim.

Ushbu ko‘rib chiqish natijalari mavjud adabiyotlar bilan solishtirilganda bir nechta moslashuv va farqlarni ko‘rsatadi. Oldingi tadqiqotlar raqamli va IT-markazlashgan sohalarda kiberxavfsizlikning ahamiyati ortib borayotganini doimiy ravishda ta’kidlagan. Ko‘pgina tadqiqotlar kiberxavfsizlikni an’anaviy xavflarni boshqarish tizimlariga integratsiyalash uchun loyiha menejerlarining xavfga yanada yaxlit yondashuvini qo‘llashlari kerakligini ta’kidlaydi. Masalan, Bannerman (2021) va Crespo & Taboada (2021) kiberxavfsizlik xatarlarini doimiy monitoring qilish zarurligini qayd etadi, bu fikr ushbu ko‘rib chiqishda ham aks etadi. Biroq, sezilarli farq signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlik uchun texnologik echimlarni qo‘llashda ko‘rinadi. Ko‘pgina tadqiqotlar xavfsiz vositalar va shifrlash texnologiyalarining ahamiyatini muhokama qilsa-da, ushbu sharh KO‘B uchun tatbiq etish muammolarini alohida ta’kidlaydi. Kichikroq tashkilotlarning cheklangan resurslari yuqori xarajatli xavfsizlik choralarini qo‘llashda to‘sqinlik qiladi, bu bo‘shliq avvalgi tadqiqotlarda kamroq ko‘rib chiqilgan. Shuningdek, tashkilot madaniyati signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlik samaradorligini belgilovchi omil sifatida muhim ahamiyatga ega ekanligi ko‘rsatildi. Natijalar shuni ko‘rsatadiki, kibertahdidlar atrofida ochiq munozaralarni qo‘llab-quvvatlovchi tashkilotlar xavflarni erta aniqlash va yumshatish imkoniga ega. Ushbu kuzatish loyihalarda signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlikdan xabardor madaniyatni shakllantirish muhimligini ko‘rsatadigan oldingi tadqiqotlarga mos keladi.

XULOSA

Ushbu ko‘rib chiqish signal va tasvirlarni qayta ishlash loyihalarida kiberxavfsizlik va loyihalarni boshqarishning muhim kesishishini ko‘rsatadi. Natijalar shuni ochib beradi-ki, loyiha menejerlari ko‘pincha kiberxavfsizlik bo‘yicha zarur bilimlardan yetishmaydi, bu esa loyihalarni raqamli tahdidlarga nisbatan zaif qilishi mumkin. Shu bilan birga, kiberxavfsizlikning

loyihalarni rejalashtirish, amalga oshirish va monitoring qilish jarayoniga erta integratsiyasi xavflarni samarali boshqarish va manfaatdor tomonlarning ishonchini oshirishda hal qiluvchi rol o‘ynaydi. Signal va tasvirlarni qayta ishlash loyihalarida ilg‘or amaliyotlar, masalan, kiberxavfsizlik bo‘yicha mutaxassislar bilan erta hamkorlik qilish, doimiy monitoring va xavfsiz texnologiyalarni qo‘llash, loyiha natijalarini sezilarli darajada yaxshilash imkonini beradi. Shu sababli, loyiha menejerlari loyiha boshlanganidan boshlab va uning butun hayoti davomida kiberxavfsizlik strategiyalarini doimiy ravishda tatbiq etishi, kichik va o‘rta korxonalar hamda cheklangan resurslarga ega tashkilotlar uchun amaliy yechimlarni ishlab chiqishi zarur. Bu yondashuv nafaqat xavflarni kamaytiradi, balki signal va tasvirlarni qayta ishlash loyihalarining muvaffaqiyatini mustahkamlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR:

Abbott, K. (2020). Keng ko'lamli loyihalarda kiberxavfsizlikni boshqarish. Loyiha boshqaruvi xalqaro jurnali,
38(2), 133–150.
Adams, B. (2020). Loyihalarda masofaviy ish kiberxavfsizlik muammolari. Kiberxavfsizlik jurnali, 6(1), 301–318.
Ahmad, A., Maynard, SB, & Park, S. (2014). Axborot xavfsizligi strategiyalari: tashkiliy ko'p strategiyali istiqbolga.
Intelligent Manufacturing jurnali, 25(4), 791–802. https://doi.org/10.1007/s10845-012- 0683-0
Alotaybi, F. (2023). Loyihani boshqarishda kiberxavfsizlik risklari: tanqidiy sharh. Kompyuterlar va xavfsizlik, 126, 233–251.
Anderson, R. (2018). Loyiha menejerlari uchun kiberxavfsizlik: Strategiyalar va eng yaxshi amaliyotlar. Loyiha boshqaruvi jurnali, 49(4), 5–20.
Archer, T. va Li, M. (2021). Agile loyiha boshqaruvida kiberxavfsizlikni integratsiyalash. Axborot xavfsizligi va ilovalari jurnali, 58, 45– 62.
Arksey, H. va O'Malley, L. (2005). Ko'lamli tadqiqotlar: metodologik asosga. Ijtimoiy tadqiqotlar metodologiyasi xalqaro jurnali, 8(1), 19-32. https://doi.org/10.1080/1364557032000119616
Bannerman, P. (2021). IT-loyihalarida kiberxavfsizlik xatarlarini bartaraf etish. Axborot va boshqaruv, 58(1), 15–30.
Baxter, P. va Chen, Y. (2020). KO'K kiberxavfsizlik asoslari: strategik amalga oshirish uchun qiyosiy tahlil. Kiberxavfsizlik jurnali, 12(3), 55–70.
Bechara, R. (2022). Aqlli shahar loyihalarida IoT xavfsizligi.
Barqaror shaharlar va jamiyat, 87, 45–63.
Braun, M. (2022). Qurilish loyihalarini boshqarishda kiberxavfsizlik. Qurilishda avtomatlashtirish, 137, 211–228.