SH.R. GULOMOV, F.B. BOTIROV, Z.I. AZIZOVA

HUJUM INSIDENTLARI VA UNGA REAKSIYA

O‘ZBEKISTON RESPUBLIKASI OLIY VA O‘RTA MAXSUS TA’LIM VAZIRLIGI

O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

SH.R. GULOMOV, F.B. BOTIROV, Z.I. AZIZOVA

HUJUM INSIDENTLARI VA UNGA REAKSIYA

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligining Muvofiqlashtiruvchi kengashi tomonidan o‘quv qo‘llanma sifatida tavsiya etilgan

«Mahalla va oila nashriyoti»
Toshkent – 2021

UDK: 004:007(075)
G 95

Gulomov, Sh.R., Botirov,F.B., Azizova, Z.I. Hujum insidentlari va unga reaksiya [Matn] : o'quv qo'llanma / Sh.R. Gulomov, F.B. Botirov, Z.I. Azizova .-Toshkent : Mahalla va Oila,2021.-164 b.

UO'K 004:007(075)

O‘quv qo‘llanma axborot xavfsizligi hodisalarini samarali yo‘l bilan aniqlash va hal qilish, xususan ularni qachon axborot insidenti sifatida tasniflash lozimligi haqida qaror qabul qilish, aniqlangan axborot xavfsizligi insidentlarini baholash va ularga nisabatan eng maqbul va samarali tarzda chora ko‘rish xususida ma’lumotlarni ifodalagan «Hujum insidentlari va unga reaksiya» nomi ostidagi fan bo‘limiga bag‘ishlangan.

O‘quv qo‘llanma 5330300 - «Axborot xavfsizligi» yo’nalishi bo‘yicha ta’lim olayotgan bakalavriatura talabalari uchun tavsiya etiladi, hamda faoliyati axborot xavfsizligini ta’minlash, hujum insidentlari va unga reaksiya bilan bog‘liq bo‘lgan mutaxassislarning keng doirasi uchun ham foydali bo‘lishi mumkin.

Taqrizchilar:

Zaynutdinova M.B. – Muhammad al – Xorazmiy nomidagi TATU, “Axborot texnologiyalari” kafedrasi dotsenti, t.f.n.

Allaberganov B.A. – O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi, yetakchi mutaxassis.

ISBN 978-9943-7779-2-7

MUNDARIJA

KIRISH 8

1.AXBOROT XAVFSIZLIGI INSIDENTLARI TUSHUNCHASI, VAZIFALARI VA VOSITALARI 12

1.1 Axborot xavfsizligi insidentlarini boshqarishning asosiy tushunchalari 12

1.2 Axborot xavfsizligi insidentlarini boshqarishning maqsad va vazifalari 15

1.3 Axborot xavfsizligi insidentlarini boshqarish tizimi 19

1.4 Axborot xavfsizligi insidentlarini boshqarishni qurish jarayonlari 22

Asosiy xulosalar 26

Nazorat savollari 27

2.AXBOROT XAVFSIZLIGI INSIDENTLARINI BOSHQARISHDA NORMATIV BAZALAR 28

2.1 O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016): standartiga muvofiq axborot xavfsizligi insidentlarini boshqarish bosqichlari 28

2.2 Axborot xavfsizligi insidentlarini boshqarish siyosati 30

2.3 Axborot xavfsizligi insidentlarini boshqarishning meyoriy asoslari 33

2.4 Axborot xavfsizligi insidentlarini boshqarishni rejalashtirish va tayyorgarlik ko‘rish 35

2.5 Axborot xavfsizligi insidentlarini identifikasiyalash va baholash mezonlari 36

Asosiy xulosalar 43

Nazorat savollari 43

3.AXBOROT XAVFSIZLIGI INSIDENTLARI VA HODISALARI TO‘G‘RISIDAGI HISOBOT 44

3.1 Axborot xavfsizligi insidentlari va hodisalari to‘g‘risidagi hisobot 44

3.2 Axborot xavfsizligi insidentlari va hodisalari qayta ishlash.. 45

3.3 Axborot xavfsizligi insidentlarini guruhlarga ajratish 47

3.4 Axborot xavfsizligi insidentlarini nazorat etuvchi vositalarning tahlili 51

3.5 Jarayonlar o‘rtasida rollarni taqsimlash va insidentni boshqarish jarayonidagi xodimlarni aniqlash 58

3.6 Axborot xavfsizligi insidentlarini presedentli tahlili 63

3.7 Axborot xavfsizligi insidentlarini boshqarish dasturlari..... 72
Asosiy xulosalar..... 78
Nazorat savollari..... 79
4.AXBOROT XAVFSIZLIGI INSIDENTLARINI TADQIQ QILISH..... 80
4.1 Insidentlarni tadqiq qilish bosqichlari..... 80
4.2 Insidentni toifalash va klassifikasiyasi..... 87
4.3 Insidentni tadqiq qilish elementlari..... 88
Asosiy xulosalar..... 91
Nazorat savollari..... 91
5.AXBOROT XAVFSIZLIGI INSIDENTLARINING TERGOVI..... 92
5.1 Korxonada axborot xavfsizligi insidentlarini tergov qilish.. 92
5.2 Axborot xavfsizligi insidentlari tergovida guruhlar tuzilmasining modellari..... 99
5.3 Axborot xavfsizligi insidentlarini tergov qilish jarayonidagi qarshiliklar..... 102
5.4 Korxonada axborot xavfsizligi insidentlarini baholash usullari..... 104
Asosiy xulosalar..... 110
Nazorat savollari..... 110
6.AXBOROT XAVFSIZLIGI INSIDENTLARIGA JAVOB QAYTARISH..... 111
6.1 Axborot xavfsizligi insidentlariga javob qaytarishni hayot davri prosedurasi..... 111
6.2 Axborot xavfsizligi insidentlariga javob qaytarish guruxi.... 131
6.3 Axborot xavfsizligi insidentlariga javob qaytarishning asosiy bosqichlari..... 138
6.4 Axborot xavfsizligi insidentlari sohasida o'qitish va xabardor etishni ta'minlash..... 143
Asosiy xulosalar..... 149
Nazorat savollari..... 150
ADABIYOTLAR RO'YHATI..... 151
BELGILAR VA QISQARTMALAR..... 153
TERMINLAR LUG'ATI..... 155

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 8
1. СРЕДСТВА, ЗАДАЧИ И ПОНЯТИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 12
1.1 Базовое понимание инцидентов информационной безопасности 12
1.2 Цель и задачи управления инцидентами информационной безопасности 15
1.3 Система защиты информации при управлении инцидентами 19
1.4 Процессы построения управления инцидентами информационной безопасности 22
Основные выводи 26
Контрольные вопросы 27
2. НОРМАТИВНЫЕ ОСНОВЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 28
2.1 Стадии управления инцидентами информационной безопасности с соответствием стандарту O'z DSt 3386: 2019 (ISO / IEC 27035-1: 2016) 28
2.2 Политика управления инцидентами информационной безопасности 30
2.3 Нормативная база инцидентов информационной безопасности 33
2.4 Подготовка и планирование инцидентов информационной безопасности 35
2.5 Критерии оценки и выявления инцидентов информационной безопасности 36
Основные выводи 43
Контрольные вопросы 43
3. ОТЧЁТ ОБ СОБЫТИЕ И ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 44
3.1 Отчет о событиях и инцидентах информационной безопасности 44
3.2 Обработка событий и инцидентов информационной безопасности 45
3.3 Группировка инцидентов информационной безопасности 47
3.4 Анализ управления инцидентами информационная

безопасность 51
3.5 Распределение ролей между процессами и идентификация персонала в процессе управления инцидентами 58
3.6 Прецедентный анализ инцидентов информационной безопасности 63
3.7 Программное обеспечение для управления инцидентами информационной безопасности 72
Основные выводи..... 78
Контрольные вопросы 79
4.ИССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 80
4.1 Этапы расследования происшествия 80
4.2 Классификация происшествий 87
4.3 Элементы расследования инцидента 88
Основные выводи..... 91
Контрольные вопросы 91
5. РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 92
5.1 Расследование инцидентов информационной безопасности на предприятии..... 92
5.2 Модели групповой структуры при расследовании инцидентов информационной безопасности 99
5.3 Сопротивление при расследовании инцидентов информационной безопасности 102
5.4 Методы оценки инцидентов информационной безопасности на предприятии 104
Основные выводи..... 110
Контрольные вопросы 110
6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 111
6.1 Жизненный цикл процедура реагирования на инциденты информационной безопасности 111
6.2 Группа реагирования на инциденты информационной безопасности 131
6.3 Основные этапы реагирования на инциденты информационной безопасности 138
6.4 Обеспечить обучение и информацию в области инцидентов информационной безопасности 143

Основные выводи..... 149
Контрольные вопросы 150
СПИСОК ЛИТЕРАТУРЫ..... 151
ЗНАКИ И СОКРАЩЕНИИ..... 153
СЛОВАРЬ ТЕРМИНОВ..... 155

KIRISH

Butun dunyo bo'ylab axborot texnologiyalari va juda tezlik bilan rivojlanishi natijasida bir necha yuzlab yangi imkoniyatlar yaratilmoqda. Har bir yaratilgan imkoniyat jamiyatdagi barcha insonlar uchun foyda keltirishi bilan bir qatorda ularni yaratilgan imkoniyatlardan to'g'ri foydalanishi uchun axborot texnologiyalari bo'yicha yetarli bilim va ko'nikmaga ega bo'lishlarini talab etadi. Chunki yaratilgan imkoniyatlardan hamma ham bir xil ezgu maqsad yo'lida foydalanmasligi mumkin. Shuning uchun axborot texnologiyalari foydalanuvchilarining barchasidan axborot xavfsizligi bo'yicha hech bo'lmaganda boshlang'ich bilimga ega bo'lishi kerak. Agar foydalanuvchi o'zining shaxsiy tarmog'idan foydalangan holda biror bir xatolikka yo'l qo'ysa zarar kata qismi o'z zimmasiga tushadi, lekin foydalanuvchu tashkilot tarmog'idan foydalangandan aynan shunday xatolikka yo'l qo'ysa unda zararni tashkilot ko'radi. Axborot xavfsizligi mutaxassislariga ma'lumki axborot xavfsizligini (AX) boshqarish siyosati va vositalari o'z holicha axborot, axborot tizimlari, xizmatlari yoki tarmoqlarini to'liq himoya qilinishini kafolatlamaydi. Boshqarish vositalari amalga oshirilgach, zaifliklar yuzaga kelishi va ular AX samaradorligi pasayishiga va AX insidentlari sodir bo'lishiga sabab bo'lishi mumkin. Mazkur holat tashkilotning biznes-jarayonlariga bevosita va bilvosita salbiy ta'sir qilishi mumkin. Bundan tashqari, oldin identifikatsiya qilinmagan yangi turdagi xavflar paydo bo'lishi muqarrar. Tashkilot bunday insidentlarni hal qilishga etarli darajada tayyor bo'lmasligi ularga nisbatan javob choralari etarlicha samarali bo'lmasligiga olib keladi va tashkilot faoliyatiga potentsial salbiy ta'sirni kuchaytiradi. Oqibatda samarali AX dasturidan manfaatdor bo'lgan har qanday tashkilot quydagilarga etiborini kuchaytiradi:

- AX insidentlarini aniqlash, ular bo'yicha hisobot tuzish va baholashga;
- AX insidentlariga nisbatan chora ko'rish, shu jumladan insidentlarning oldini olish, kamaytirish va nohush oqibatlaridan so'ng tiklanish uchun tegishli vositalarni ishga tushirishga;
- AXdagi zaifliklarni baholash va echimini topish bo'yicha tegishli choralar ko'rish uchun ular bo'yicha hisobotga;
- AX insidentlari va zaifliklaridan dars olish, oldini oluvchi boshqaruv vositalarini joriy etishga strukturalangan va rejalashtirilgan

yondashuvga ega bo‘lishi va AX insidentlarini boshqarishga umumiy yondashuvni takomillashtirishi lozim.

Bunday rejalashtirilgan yondashuvga erishish maqsadida standartlar AX insidentlarini boshqarish jihatlari bo‘yicha qo‘llanmalarni taqdim etadi, jumladan:

- O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) (mazkur standart). Unda AX insidentlariga doir asosiy tushunchalar va ularni boshqarishning asosiy bosqichlari, insidentlarni boshqarishni yaxshilash usullari bayon etilgan. Mazkur standart ushbu tushunchalarni insidentlarni aniqlash, ular bo‘yicha hisobot tayyorlash, baholash va chora ko‘rishga, orttirilgan tajribani qo‘llashga strukturalangan yondashuv bilan birlashtiradi;
- O‘z DSt 3367:2019 (ISO/IEC 27035-2:2016, MOD) standartida insidentlarga nisbatan javob choralarini qanday rejalashtirish va ko‘rish bayon etilgan. Bu qism “Rejalashtirish va tayyorganlik ko‘rish” hamda “Orttirilgan tajriba” bosqichlarini o‘z ichiga oladi.

Standartlar AX insidentlari yuzasidan taftish o‘tkazish va taftish o‘tkazishga tayyorgarlik ko‘rish bo‘yicha qo‘llanma vazifasini o‘taydigan boshqa hujjatlarni to‘ldirishga xizmat qiladi. Standartlar to‘liq qo‘llanma hisoblanmaydi, balki vosita, usul va uslublar lozim tarzda tanlanishini ta’minlaydigan ma’lum asosiy printsplarga hamda zarurat bo‘lganda maqsadga erishish uchun ularning yaroqliligidan dalolat berishga tayanadi.

Mamlakatimizda axborot texnologiyalarining rivojlanishi bilan bir qatorda xo‘jalik va davlat boshqaruvi organlarida hujum insidentlariga alohida e’tibor qaratilmoqda. Shu sababli ma’lumotlarni qayta tiklash, ma’lumotlarni va ma’lumot tashuvchilarni kompyuter ekspertizasi bo‘yicha sezilarli natijalarga erishildi hamda axborot xavqsizligi insidentlariga qarshi reaktsiya rejasi va tergov bosqichlarini yaratish boshlandi. O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoevning 2017 yil 8 fevraldagi “Qonun hujjatlarini tarqatish tizimini tubdan takomillashtirish chora-tadbirlari to‘g‘risida”gi qarorida va 2017-2021 yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida vazifalar belgilab olindi, shular qatorida «...axborot xavfsizligini ta’minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish» va axborot xavfsizligi insidentlarini boshqarishni rejalashtirish masalalariga alohida e’tibor qaratilgan. Bu vazifalarni amalga oshirish eng muhim muammolardan biri hisoblanadi.

Mazkur o‘quv qo‘llanma axborot xavfsizligi insidentlarini boshqarishni qurish jarayonlari va ularning normativ bazalari, axborot xavfsizligi insidentlari va hodisalarini qayta ishlash, axborot xavfsizligi insidentlarining tergovi va axborot xavfsizligi insidentlariga javob qaytarishning nazariy va amaliy asoslarini o‘z ichiga oladi.

Qo‘llanmaning birinchi bobida axborot xavfsizligi insidentlarini boshqarishning maqsad va vazifalari, ko‘rinishlari va asosiy tushunchalari, axborot xavfsizligi insidentlarini boshqarish tizimi va axborot xavfsizligi insidentlarini boshqarishni qurish jarayonlari ko‘rib chiqilgan. Axborot xavfsizligi insidentini boshqarishning xayot davri, axborot xavfsizligi insidentlarini olidini olishni hujjatlashtirish, insidentlarni bartaraf etish bo‘ycha asosiy echimlar keltirilgan.

Ikkinchi bobda axborot xavfsizligi insidentlarini boshqarish bosqichlari, siyosati, meyoriy asoslari, axborot xavfsizligi insidentlarini boshqarishni rejalashtirish, identifikatsiyalash va baholash mezonlari axborot xavfsizligi insidentini boshqarish ko‘rib chiqilgan, hamda insident faktorlarida inson omili va insidentlarning ta’sir doirasini aniqlash yo‘llari keltirilgan.

Qo‘llanmaning uchinchi bobida axborot xavfsizligi insidentlari va hodisalari to‘g‘risida hisobot tayyorlash va ularni qayta ishlash, axborot xavfsizligi insidentlarini guruhlarga ajratish va prentsedentli tahlili hamda axborot xavfsizligi insidentlarini boshqarish dasturlari keltirilgan. Axborot xavfsizligi insidentlarini boshqarishda yuzaga keladigan muammolar, pretsedentli taxlilni qo‘llash kontseptsiyasi va uning mantiqiy tuzilishi bilan bir qatorda boshqarish sxemasini testdan o‘tkazish yo‘llari ko‘rsatib o‘tilgan.

To‘rtinchi bob insidentlarni boshqarishdagi murakkabliklar, hujum oqibatlari, sabablari va ularning paydo bo‘lish yo‘llarini aniqlanuvchi insidentlarni tadqiq qilish masalalarini ko‘rib chiqishga bag‘ishlangan. Insident toifalari va klassifikatsiyasi hamda axborot xavfsizligi insidentlarini namunaviy tahlillash tadqiq qilinadi.

Beshinchi bobda korxonada axborot xavfsizligi insidentlarini tergov qilish, tergov qilish guruhlarining modellari, tergov qilish jarayonidagi qarshiliklar va korxonada axborot xavfsizligi insidentlarini baholash usullari keltirib o‘tilgan. Javob qaytarish guruhining tuzilmasini asosiy uch xil modeli markazlashtirilgan model, taqsimlangan model, korporativ modellarning afzalliklari va kamchiliklari qiyosiy tahlil qilish orqali kerakli ma’lumotlar berilgan. Axborot xavfsizligi insidentlarini qayta ishlashni boshqarish jarayoni va

axborot xavfsizligi insidentlarini uning omillari asosida baxolash usullari hamda axborot xavfsizligi insidentlarini baholashning bloksxemasi keltirilgan.

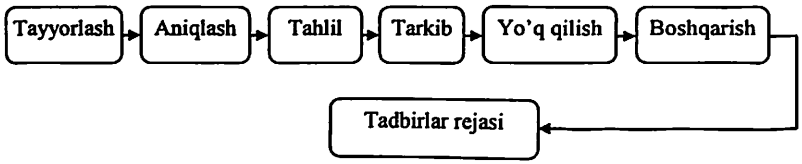
Oltinchi bob axborot xavfsizligi insidentlariga javob qaytarishni hayot davri protsedurasi, javob qaytarish guruhi, javob qaytarishning asosiy bosqichlari va axborot xavfsizligi insidentlari sohasida o'qitish va xabardor etishni ta'minlash bilan bir qatorda tashkiliy ishlar ko'rib chiqilgan.

O'quv qo'llanma 5330300 - «Axborot xavfsizligi» yo'nalishi bo'yicha ta'lim olayotgan bakalavriatura talabalari uchun tavsiya etiladi, hamda faoliyati axborot xavfsizligini ta'minlash, hujum insidentlari va unga reaksiya bilan bog'liq bo'lgan mutaxassislarning keng doirasi uchun ham foydali bo'lishi mumkin.

1. AXBOROT XAVFSIZLIGI INSIDENTLARI TUSHUNCHASI, VAZIFALARI VA VOSITALARI

1.1. Axborot xavfsizligi insidentlarini boshqarishning asosiy tushunchalari

Axborot xavfsizligi insidenti – bu axborot xavfsizligi tizimidagi bir yoki bir necha tasodifiy va kutilmagan hodisalar, ish jarayonlarini tahlil qilishga katta imkoniyat berish va axborot himoyasini tahdidga qo'yilishi bilan bir qatorda axborot xavfsizligi tizimiga amalga oshiriladigan hodisalar, axborot xavfsizligiga kutilgan va kutilmagan tahdidlar yig'indisidir. Bu jarayonni tasavvur qilish uchun axborot xavfsizligi insidentini boshqarishning hayotiy davrini ketma ketligiga e'tibor qaratish kerak.



1.1-rasm. Axborot xavfsizligi insidentini boshqarishning xayot davri

Action Plan (Tadbirlar rejasi) – bu insidentlarga qarshi chora-tadbirlarni umumiy rejasi.

Prepare (Tayyorlash) - bu ma'lumotlarni saqlash va insidentga javob qobiliyatini takomillashtirish (rejalashtirish va tayyorlash).

Detect (Aniqlash) - bu ma'lumotlarni saralash va o'rganish jarayonida insidentlarni aniqlash.

Analyze (Tahlil qilish) – bu jarayon va ma'lumotlarni nazorat qilish, tahlil qilish, kuzatish va qayta tiklash.

Contain (Saqlash) - bu zararlarni kamaytirish, axborotni o'g'irlashdan himoyalash, xizmat ko'rsatishdagi o'z ulushlarini nazoratlash.

Eradicate (Barham berish) – bu tizimga nisbatan tahdidlarni bartaraf etish.

Recover (Qayta tiklash) – bu xavfsiz va tezkorlik bilan hisoblash tizimlarini qayta tiklash va h.k.z.

Manage (Boshqarish) – bu insidentlarni boshqarish jarayoni.

Axborot xavfsizligi insidentlarini boshqarishda ISO/IEC 27035:2016 standartining o'rni juda muhim ahamiyat kasb etadi.

Ushbu standart ikki qismdan iborot bo'lib, 1-Qism: Insidentni boshqarish prinsiplari, 2-Qism: Insidentga javob qaytarishni rejalashtirish va tayyorlash bo'yicha qo'llanma hisoblanadi.

ISO/IEC 27035-1:2016, 1-Qism: Insidentni boshqarish prinsiplari.

ISO/IEC 27035 standartning ushbu qismi bir necha qismlardan tashkil topgan butun xalqaro standart uchun asos bo'lib hisoblanadi. Unda AX insidentlari tushunishda va boshqarishda asosiy tushunchalarni aniqlashtirib,ularning aniqlanishida strukturali yondashuv prinsiplarini, axborotlashtirishni, baholashni, o'z vaqtida reaksiya ko'rsatishni hamda tajribalarda xulosa chiqarish tushunchalarini qamrab olgan. Standartda keltirilgan prinsiplar umumiy hisoblanib, tashkilotlarning turi, hajmi va xarakteridan qat'iy nazar foydalanishlari mumkin. Tashkilotlar o'zlarining turi, hajmi va xarakteridan kelib chiqqan holda AX insidentlari xavf hatarlariga qarshi choralarni standartda keltirilgan ko'rsatmalar asosida moslashtirishlari mumkin. Bu standart AX insidentlari menejmenti xizmatini ko'rsatuvchi tashqi tashkilotlar tomonidan ham ishlatilishi mumkin.

ISO / IEC 27035-1: 2016 ko'p qismli xalqaro standart hisoblanadi. Bu standartda axborot xavfsizligi insidentlarini boshqarishni etaplari va asosiy tushuchalari, insidentlarga javob qaytarish va baholashlari ko'rsatib o'tilgan.

ISO / IEC 27035-1: 2016 standartida keltirilgan prinsiplar korxonaning xarakteri va hajmiga qaramasdan turib ham bemalol qo'llanishga mo'ljallangan.

Korxonalar ISO / IEC 27035-1: 2016 standartida keltirilgan tavsiyalarni axborot xavfsizligi xavf-xatarlarini turiga, hajmiga va xarakteriga qarab to'g'rilashlari mumkin.

ISO/IEC 27035-2:2016, 2-Qism: Insidentga javob qaytarishni rejalashtirish va tayyorlash bo'yicha qo'llanma.

ISO/IEC 27035-2 standarti AX insidentlariga reaksiya qilish bo'yicha ko'rsatmalarni o'z ichiga oladi. ISO/IEC 27035-2 standartiga ko'ra ko'rsatmalar "Rejalashtirish va tayyorlanish", "Xulosa chiqarish" etaplariga va "AX insidentlari boshqarish etaplari" modeliga asoslangan.

Standartda keltirilgan prinsiplar umumiy hisoblanib, tashkilotlarning turi, hajmi va xarakteridan qat'iy nazar foydalanishlari mumkin. Tashkilotlar o'zlarining turi, hajmi va xarakteridan kelib

chiqqan holda AX insidentlari xavf qatarlariga qarshi choralarni standartda keltirilgan ko‘rsatmalar asosida moslashtirishlari mumkin. Bu standart AX insidentlarini boshqarish xizmatini ko‘rsatuvchi tashqi tashkilotlar tomonidan ham ishlatilishi mumkin.

Axborot xavfsizligi insidentlarini boshqarishda ISO/IEC 27037 standarti ham ishlab chiqilgan.

Bu standar raqamli holda keltirilgan potensial dalillar bilan muomila qilish jarayonlariga oid aniq yo‘l-yo‘riqlarni namoyish etadi. Bu jarayonlarga quyidagilar kiradi: identifikasiya, raqamli holda keltirilgan potensial dalillarni yig‘ish, olish va saqlash. Bu jarayonlar raqamli holda keltirilgan dalillarning butunligini ta’minlashda hamda tergov qilish uchun kerak bo‘ladi. Bu standart raqamli holda keltirilmagan dalillar uchun ham umumiy yoriqnomalarni o‘z ichiga oladi. Bular esa o‘z o‘rnida raqamli holda keltirilgan potensial dalillarni tahlil qilish paytida foydali bo‘lishi mumkin.

Ushbu standart raqamli ko‘rinishda bo‘lgan dalillarning ishonchliligini aniqlovchi shaxslarni axborotlash uchun ham mo‘ljallangan. Bu standart raqamli ko‘rinishda bo‘lgan potensial dalillarning namoyish qilinishiga, tahlilga va himoyaga muhtoj tashkilotlarda qo‘llanilishi mumkin. Bu standart raqamli ko‘rinishda bo‘lgan dadillar (ko‘p hollarda katta va murakkab dadillar) bilan bog‘liq bo‘lgan, jarayonlari hosil qiluvchi va ularni baholaydigan boshqaruv organlari uchun muhim hisoblanadi.

Haqiqiy standartda ko‘rsatib o‘tilgan potensial dalillar raqamli qurilmalar, tarmoqlar, ma’lumotlar bazasi va boshqa turli raqamli vositalardan olingan bo‘lishi mumkin. Chunki bu dalillar hosil bo‘lishida yo‘q raqamli formatga ega hisoblanadi. Haqiqiy standart analogli ma’lumotlarni raqamli ma’lumotlarga o‘zgartirish muammosini qamrab olmagan.

Bu standartning qo‘llanilish sohasi kelib chiqib, raqamli ko‘rinishda bo‘lgan dalillar(bularga identifikasiya, raqamli holda keltirilgan potensial dalillarni yig‘ish, olish va saqlash kiradi) bilan muomila qiladigan aniq sohalar to‘grisida yuriqnomalarni qamrab olgan. Haqiqiy standart raqamli ko‘rinishdagi dalillar bilan ishlash jarayonida kelib chiqadigan keng tarqalgan holatlar bo‘yicha ko‘rsatmalarga ega. Haqiqiy standart tashkilotlarda raqamli korinishda bo‘lgan potensial dalillarning yurisdiksiyalar orasida almashinuv jarayonini yengillashtirib, intizomiy jarayonlarni amalga oshirishga hizmat qiladi.

Haqiqiy standart o'zida turli xil xolatlarda ishlatiladigan quyidagi qurilmalar va funksiyalar haqida tavsiyalar beradi:

- turli kompyuterlarda ishlatiladigan raqamli ma'lumot tashuvchilar, masalan, qattiq disk, disketalar, optik va magnitli disklar;

Mobil telefonlar, "Cho'ntak" shaxsiy kompyuterlar, shaxsiy elektron qurilmalar, xotira kartalari;

- mobil navigasion tizimlar;
- raqamli fotoapparatlar va videokameralar;
- tarmoqga ulanadigan turli kompyuterlar;
- TCP/IP protokoliga asoslangan tarmoqlar va boshqa raqamli protokollar;
- yuqorida sanab o'tilgan qurilmalar funksiyasiga asoslangan qurilmalar.

Yuqoridagi ma'lumotlardan ko'rinib turibdiki, axborot xavfsizligi insidentlari boshqarish nafaqat axborot xavfsizligi tizimiga amalga oshirilgan xodisalar balki, kutilgan va kutilmagan tahdidlar yig'indisini ham anglatadi.

1.2. Axborot xavfsizligi insidentlarini boshqarishning maqsad va vazifalari

AX umumiy strategiyasining asosiy qismi sifatida tashkilot AX insidentlarini boshqarishga strukturalangan va aniq rejalashtirilgan yondashuvni ta'minlash maqsadida boshqaruv vositalari va taomillarni joriy etishi zarur. Tashkilotning nuqtai nazaridan, asosiy maqsad – AX insidentlariga yo'l qo'ymaslik yoki insidentlar tufayli o'z faoliyatiga yetkazilishi mumkin bo'lgan bevosita va bilvosita zararni imkon qadar kamaytirish uchun AX insidentlarining ta'sirini to'xtatib turish. Axborot resurslariga yetkaziladigan zarar faoliyatga salbiy ta'sir qilishi mumkin, shunday ekan operasion va biznes-jarayonlar to'g'risida tushuncha AXni boshqarishning muayyan maqsadlarini aniqlashga katta ta'sir qilishi lozim.

Axborot insidentlarini boshqarishga strukturalangan va aniq rejalashtirilgan yondashuv maqsadlari quyidagilarni o'z ichiga olishi zarur:

1. AX hodisalarini samarali yo'l bilan aniqlash va hal qilish, xususan ularni qachon AX insidenti sifatida tasniflash lozimligi haqida qaror qabul qilish;
2. aniqlangan AX insidentlarini baholash va ularga nisabatan eng maqbul va samarali tarzda chora ko'rish;

3. insidentlarga chora ko'rish doirasida tegishli boshqaruv vositalari yordamida AX insidentlarining tashkilot va uning faoliyati uchun nohush oqibatlarini imkon qadar kamaytirish;

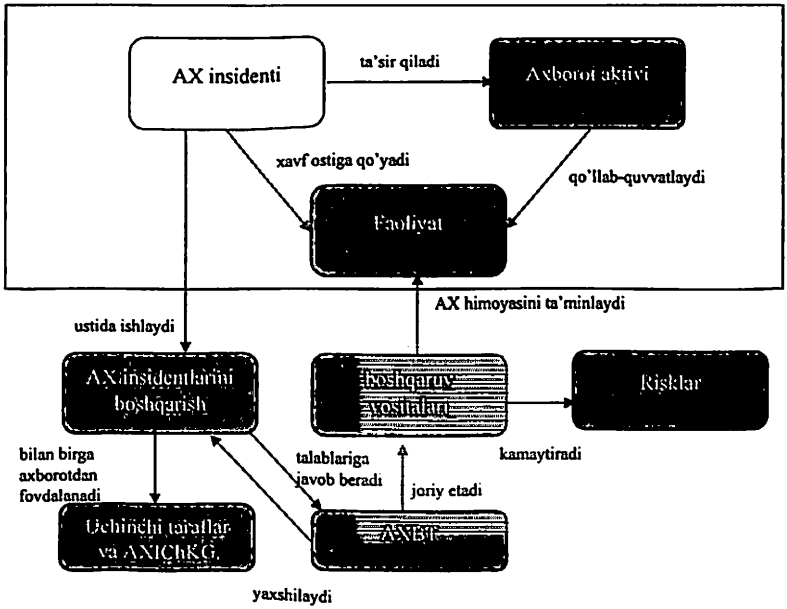
4. eskalasiya jarayoni (yuqori tashkilotlarga murojaat qilish jarayoni) orqali inqirozli vaziyatlarni boshqarish va biznes uzluksizligini boshqarishning tegishli elementlari bilan aloqa o'rnatish;

5. insidentlarning oldini olish yoki sonini qisqartirish uchun AX zaifliklarini baholash va lozim tarzda hal qilish. Baholash axborot xavfsizligi insidentlariga chora ko'rish guruhi yoki, majburiyatlar taqsimotiga muvofiq, tashkilot ichidagi boshqa guruhlar tomonidan amalga oshirilishi mumkin;

6. AX insidentlari, zaifliklar va ularni boshqarishdan tezda tajriba orttirish. Bu qayta aloqa mexanizmi AX insidenti paydo bo'lishi imkoniyatining oldini olishni, AXni boshqarish vositalarini joriy etishni va ulardan foydalanishni, AX insidentlarini boshqarish umumiy rejasini yaxshilashga xizmat qiladi.

Yuqorida bayon etilgan maqsadlarga erishish uchun tashkilotlar insidentlarni toifalarga ajratish va tasniflash bo'yicha tegishli standartlardan foydalangan holda, kelishilgan tarzda AX insidentlarini hujjatlashtirishlari va ulardan birgalikda foydalanishlari zarur. Shu tariqa miqdor ko'rsatkichlari ma'lum vaqt oralig'idagi jami ma'lumotlar asosida shakllanadi, bu esa, o'z navbatida, AXni boshqarish vositalariga investisiya kiritishda strategik qarorlar qabul qilish uchun qimmatli ma'lumotlar beradi. AX insidentlarini boshqarish tizimi tegishli uchinchitaraflar va axborot xavfsizligi insidentlariga chora ko'rish guruhi bilan axborot almashish imkoniyatiga ega bo'lishi kerak.

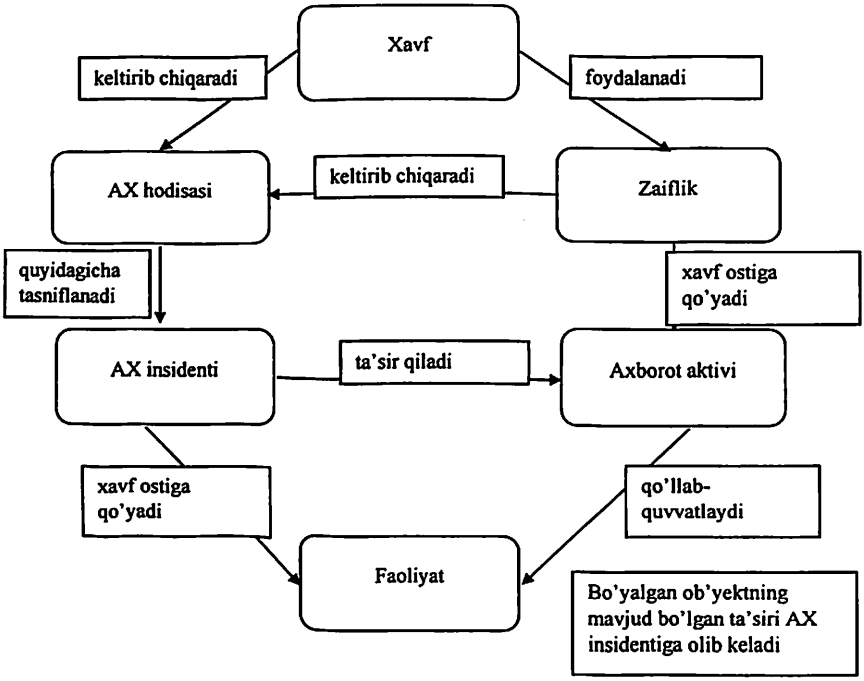
Mazkur standart bilan bog'liq bo'lgan yana boshqa bir maqsad – O'z DSt ISO/IEC 27001 standartida belgilangan va O'z DSt ISO/IEC 27002 standarti tavsiyalari bilan qo'llab-quvvatlanadigan axborot xavfsizligini boshqarish tizimiga (AXBT) qo'yiladigan talablarga muvofiq bo'lishga intiladigan tashkilotlarni qo'llanma bilan ta'minlash. O'z DSt ISO/IEC 27001 standartida AX insidentlarini boshqarish bilan bog'liq talablar bayon etilgan. Mazkur standartning V ilovasida O'z DSt ISO/IEC 27001 va O'z DSt 3386, O'z DSt 3387 standartlari o'rtasidagi muvofiqlik to'g'risida ma'lumotlar keltirilgan. AXBT o'zaro bog'liqligi 2-rasmda ko'rsatilgan. Mazkur standart, shuningdek, turli AXBTlarga qo'yiladigan talablarga ham javob berishi mumkin.



1.2-rasm. AXBT va boshqaruv vositalariga muvofiq ravishda AX insidentlarini boshqarish

AX insidentlari qasddan sodir etilgan bo'lishi (masalan, zararli dasturiy ta'minot yoki axborot tizimidan foydalanish qoidasini atayin buzish tufayli), tasodifiy bo'lishi (masalan, bexosdan sodir etilgan inson xatosi yoki oldini olib bo'lmaydigan tabiiy ofat), texnik (masalan, kompyuter viruslari tufayli) yoki notexnik sabablar (masalan, kompyuterlar yo'qotilishi yoki o'g'rilanishi) tufayli yuz berishi mumkin. Axborot ruxsatsiz oshkor etilishi, modifikasiya qilinishi, yo'q qilinishi yoki foydalanish imkoniyati yo'qotilishi, tashkilotning axborot aktivlariga zarar yetkazilishi yoki ular o'g'irlanishi insident ta'sirining oqibatlari bo'lishi mumkin.

AX insidentiga alohida misollar va ularning sabablari faqat tanishtirish maqsadida keltirilgan. Ta'kidlash lozimki, bu misollar aslo to'liq emas.



1.3-rasm. AX insidentida ob'yektlarni o'rtasidagi o'zaro bog'liqlik

Xavf axborot tizimlari, xizmatlari yoki tarmoqlarida zaifliklar bor bo'lganda yuzaga keladi, bu AX hodisalari yuzaga kelishiga olib keladi va shu tariqa potensial ravishda zaifliklarga moyilligi bo'lgan axborot aktivlarida insidentlar yuz berishiga olib keladi. 1.3-rasmda AX insidenti yuz berganda obyektlar o'rtasidagi o'zaro bog'liqlik ko'rsatilgan.

Insidentlarni boshqarishni effektiv ravishda tashkil yetish va amaliy ko'llash korxonaga quyidagi biznes ustunliklarni beradi:

- Biznes tashkilotlarga insidentlarning salbiy ta'sirini kamaytirish.
- Axborot xavfsizligini yaxshilash bo'yicha choralarni aniqlash.

Axborot xavfsizligi bo'linmalarida insidentlarni boshqarish jarayonini to'g'ri tashkil yetilishi bu:

- Barcha mutaxxasislarga rollarni va insidentlarga o'z vaqtida va sifatli reaksiya qilishni aniq taqsimlash;
- Ximoya choralari effektivligi monitoringiga tezkor axborot;

- Bo‘linmalardagi xodimlarning ishlash samaradorligini nazoratlashning shaffofligi; biznes-bo‘linmalari va axborot texnologiyalarga tegishli xodimlarning o‘zaro hamkorligi sifatini oshirish.

Insidentlarni boshkarish jarayonini avtomatlashtirish tizimi kuyidagilarni imkonini beradi:

- AX haqidagi insidentlari va xodisalarini saklash va kayta ishlash;
- ro‘y bergan insidentlarni, oldinroq ro‘y bergan insidentlar analiziga asoslanib bartaraf yetish; yig‘ilgan ma’lumotlarni tahlil qilish.

1.3. Axborot xavfsizligi insidentlarini boshqarish tizimi

Hodisalar va axborot xavfsizligi insidentlari tushunchasi.

Insident (mojoro, hodisa) - bu standart bo‘lishi mumkin bo‘lmagan hodisalar qatoriga qo‘shilmaydigan hamda xizmat holatini uzib qo‘yish yoki xizmat sifati yomonlashishi holatlariga olib keladigan har qanday hodisaga aytiladi. Axborot xavfsizligi insidenti – bu axborot xavfsizligi tizimiga amalga oshiriladigan hodisalar, axborot xavfsizligiga kutilgan va kutilmagan tahdidlar yig‘indisidir.

Axborot xavfsizligi insidentlari bilan ishlash

Bunda gap insidentlar xavfsizligi xaqida boradi. Axborot xavfsizligi rejimi o‘rnatilgandan (xujjatlar qabul qilingan, texnik qismlari o‘rnatilgan va sozlangan bo‘lib, birinchi treninglar o‘tqazilgan) so‘ng eng ko‘p vaqt insidentlar bilan ishlashga ketadi.

Insedentlar haqida ma’lumot berish

Birinchi bo‘lib insedent xaqida ma’lumot olish lozim. Bu xaqda xavfsizlik siyosatini ishlab chiqish va xodimlar uchun axborot xavfsizligi insedentlari bo‘yicha amaliy qo‘llanmani tayyorlashni o‘ylab ko‘rish lozim.

Axborotning asosiy manbalari:

1. Helpdesk.

Qurilma ishidagi har qanday muammolar vujudga kelganda sizning IT-xizmat xelpdesk ga yozishadi yoki qo‘ng‘iroq kilishadi. Shuning uchun oldindan biznes-jarayonga xelpdesk ni “biriktirib” ko‘yish va AX bo‘limiga yuboriladigan insendentlar turini ko‘rsatish lozim.

2. Foydalanuvchilardan kelgan to‘g‘ridan-to‘g‘ri xabarlar.

Yagona kontakt markazini tashkil etib, bu xaqda AX treningda xodimlarga etish lozim. Hozirgi kunda tashkilotlardagi AX bo‘limlari

unchalik kaatta emas, shuning uchun insidentlarni qabul qilishga ma'sul xodim tayinlash qiyin bo'lmaydi.

3. AX xodimlari tomonidan aniqlangan insidentlar.

Bunda xammasi oddiy va bu kabi qabul kanalini tashkil etishda jismoniy xarakat talab etilmaydi.

4. Jurnallar va ogoxlantirish tizimlari.

Antivirus konsoli, IDS, DLP va boshqa xavfsizlik tizimlarida ogoxlantirishni sozlang. Tashkilotga o'rnatilgan aggregatorlardan foydalanish qulayroq xisoblanadi. Aggregatorlar tizim va dastur loglaridan ma'lumotlar yig'adi. Tashqi tarmoqqa ulangan joylarga aloxida e'tibor berish lozim.

Boshqarish funksiyasi va mohiyati

Xozirgi paytda xalqaro amaliyotda AX insidentlarni boshqarishga oid yetarlicha normativ xujjatlar ishlab chiqilgan. Insidentlarni boshqarish savollari nafaqat AX doirasida balki butun IT-servis kelib chiqadi. ISO 20000:2005 xalqaro standartlarning Service Delivery and Support bo'limida IT-infrastrukturada inyidentlarni boshqarishni tashkillashtirishga oid bir qancha talablar keltirilgan. Ushbu standartga ko'ra insident deb "xizmat funksionalligining normal elementi xisoblanmaydigan va bu bilan xizmat sifatini pasayishiga olib keladigan har qanday hodisa" tushuniladi.

A.13 Axborot xavfsizligi insidentlarini boshqarish

A.13.1.1 Axborot xavfsizligi hodisalari haqidagi xabar. Ushbu xabar ma'lum mo'ljallangan boshqaruv kanallari orqali iloji boricha tez yuborilishi kerak

A.13.1.2 Xavfsizlikning zaifliklari haqidagi xabar. Barcha informasion tizimga taaluqli bo'lgan xodimlarni, ishchilarni va boshqa xodimlarni kuzatilayotgan zaifliklarni kuzatib borib ular haqida xabar berishlarini ta'minlash

A.13.2.1 Jarayonlar va javobgarlik. Bunda boshqarmalarga javobgarlik yuklanishi kerak bo'lib , axborot xavfsizligi insidentlariga qarshi to'g'ri, effektiv va tezkor chora ko'rish jarayonini taminlashni aniqlashtirish.

A.13.2.2 Axborot xavfsizligi insidentlaridan xulosa chiqarish. Bunda axborot xavfsizligi insidentlarining xajmi o'lchash, uning tipini aniqlash va qiymatini aniqlovchi mexanizmlarni amalga oshirish tushuniladi.

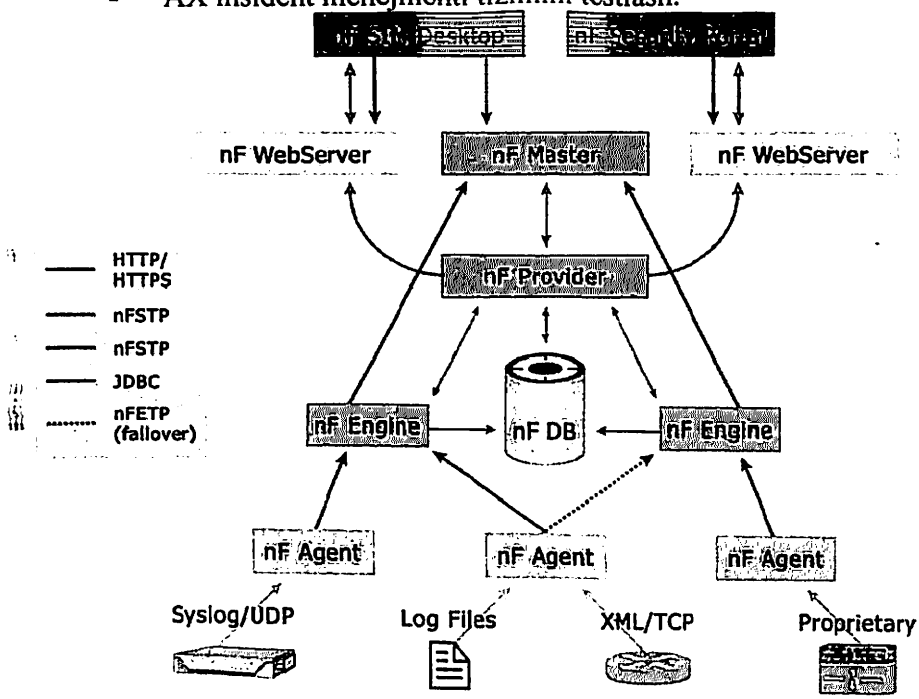
A.13.2.3 Dalillarni yig'ish. Axborot xavfsizligi insidenti sifatida biror bir shaxs yoki tashkilotlar qaraladigan bo'lsa huquqni muxofaza

qilish organlariga dalillarni yig'ish , saqlash va taqdim etish lozim bo'ladi.

AX insidentlarini boshqarish etaplari

Rejalashtirish va tayorgarlik ko'rish:

- AX insident menejmenti siyosati va bosh raxbariyatning undagi majburiyatlari;
- AX insidentini boshqarish tizimi;
- korporativ xavfsizlik va xavfsizlik tizimi, tahlil va xavf-xatarlarni boshqarish, AX siyosatini yangilash;
- AX insidentlari haqida ko'rsatmalar berish va o'rgatish;
- AX insident menejmenti tizimini testlash.



1.4-rasm. NetForensics dasturi uzluksiz ravishda xavfsizlik hodisalarini ko'rsatib beradi, kayta ishlaydi va yig'adi

Qo'llanilishi:

- AX hodisalarini aniqlash va ular haqida xabar berish;
- baholash va xulosa chiqarish: Ushbu hodisa insidentmi yoki yoq;

- AX insidentiga qonuniy ekspertiza asosida reaksiya qilish.

Tahlil:

- qo'shimcha qonuniy ekspertiza;
- yig'ilgan tajribani umumlashtirish;
- xavfsizlikni yaxshilash metodlarini aniqlash;
- AX insidentlarini boshqarish tizimini yaxshilash usullarini aniqlash.

Yaxshilash:

- menejment analizi va xavfsizlik riski analizi natijalarini qayta aniqlashtirish;
- AX insidentlarini boshqarish tizimini yaxshilash choralarni o'tkazish..

NetForensics axborot xavfsizligini boshqarish tizimi axborot xavsizligini geterogen muxitida taminlash vositalari bilan ishlash uchun mo'ljallangan. U uzluksiz ravishda xavfszlik hodisalarini ko'rsatib beradi, kayta ishlaydi va yig'adi.

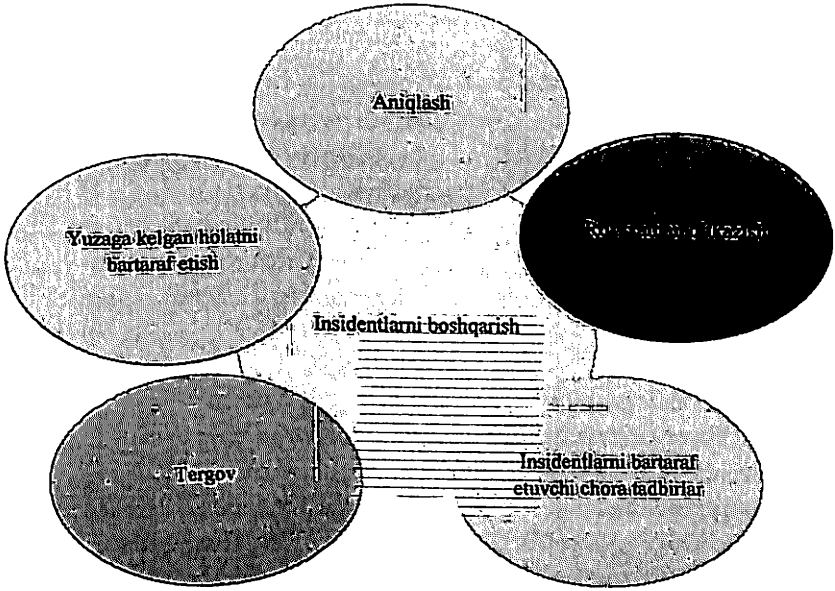
1.4. Axborot xavfsizligi insidentlarini boshqarishni qurish jarayonlari

Insident (insident)- bu standart operasiyalar qatoriga qo'shilmaydigan hamda xizmat holatini uzib qo'yish yoki xizmat sifati yomonlashishi holatlariga olib keladigan har qanday insidentga aytiladi (1.5-rasm).

Insidentni boshqarish - biznes jarayonlarni olib borish jarayonida ish holatini tezda minimal xavf bilan normal ish holatiga qaytarish faoliyati hisoblanadi, hamda qisqa davom etadigan va bir maqsad sari yo'naltirilgan xizmatlar qatoriga kiradi.

Insidentni boshqarish bo'yicha ko'p standartlar mavjud. Ular orasidan quyidagilarni keltirib o'tish mumkin:

1. ISO/IEC 27001:2013 Information security management system. Requirements. Bu standart doirasida axborot xafsizligi tizimlarini qurish uchun umumiy talablar va shu bilan birga insidentlar tizimini boshqarish uslublari keltiriladi.
2. ISO/IEC TR 18044 Information security incident management. Ushbu hujjat PDCA siklik modeli doirasida insidentlarni boshqarish infratuzilmasini tasniflaydi. Ushbu standart ichida insidentlarni boshqarish jarayonini tashkil qilishni rejalashtirish, ishga tushirish, tahlil va boshqa holatlar to'liq holda hujjatlashtirib keltirilgan.



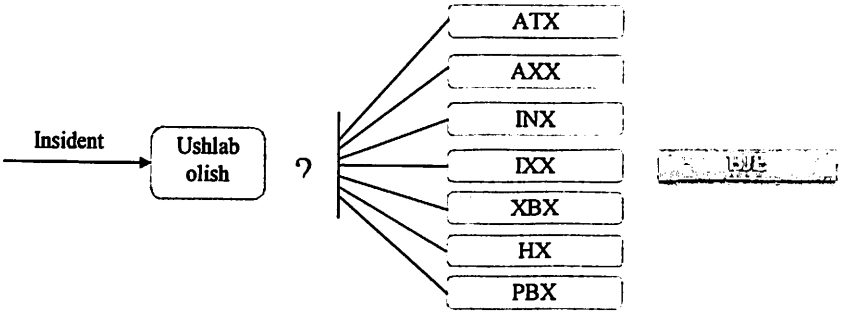
1.5-rasm. Axborot xavfsizligi insidentlari

3. CMU/SEI-2004-TR-015 Defining incident management processes for CISRT. Ushbu hujjat rejalashtirish, ishga tushirish jarayonining metodologiyasi hisoblanadi. CISRT (Critical Incident Stress Response Team). Ushbu tizimda insidentlar yuz berishini bartaraf etish, unga javob qaytarish va xafsizlikni ta'minlash jarayonlari asos qilib olinadi.

4. NIST SP 800-61 Computer security incident handling guide. Ushbu "eng yaxshi amaliyotlar" to'plami insidentlarni boshqarish jarayonlarini tashkil qilish va javob qaytarish uchun qo'llanma hisoblanadi. Har hil turdagi xavflar uchun to'laqonli javob qaytarish harakatlari hujjatlashtiriladi.

5. GOST R ISO/MEK 18044 Manaqgement information security incident. Insidentlarni boshqarish bo'yicha axborot xafsizligi bo'limi boshqaruvchilariga hamda tarmoq mutaxassislariga maslahatlar beradi.

Insidentlarni aniqlash bu murakkab jarayondir. Xodimlar bunday holatlarni bilganlari uchun, bunday insidentlarni oldini olishga aniq ketma-ket harakatlar qilishi zarur (1.6-rasm).

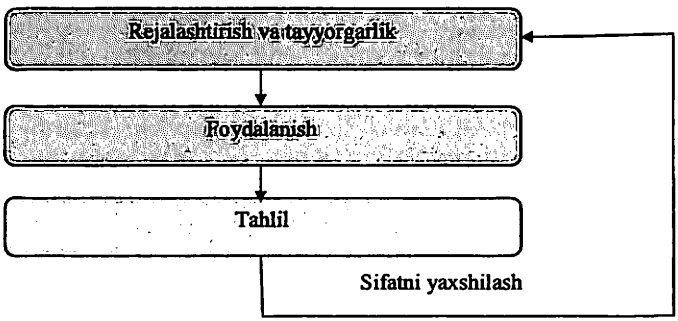


1.6-rasm. Axborot xavfsizligi insidentlarini aniqlash

1. Axborot texnologiyalari xizmati (ATX).
2. Axborot xavfsizligi xizmati(AXX).
3. Ichki nazorat xizmati (INX).
4. Huquqiy xizmat (HX).
5. Iqtisodiy xavfsizlik xizmati (IXX).
6. Xavflarni boshqarish xizmati (XBX).
7. Personalni boshqarish xizmati (PBX).
8. Biznes jarayonlar egasi (BJE).

Bunday holatlarda aniq qandaydir ko'rsatmalar yoki xodim yetarlicha malakaga ega bo'lmasa insidentga javob qaytarish ancha muammoli holat bo'lib chiqadi. Ba'zi holatlarda bir xodim bajarishi kerak bo'lgan holatlarni bir nechta xodimlarga bo'lib tashlanadi, natijada ular parallel harakat qilib faqat vaqt yo'qotishadi.

Kelishilgan holatda ishlash uchun barcha xodimlarni aniq ishga yo'naltirish lozim (1.6-rasm).



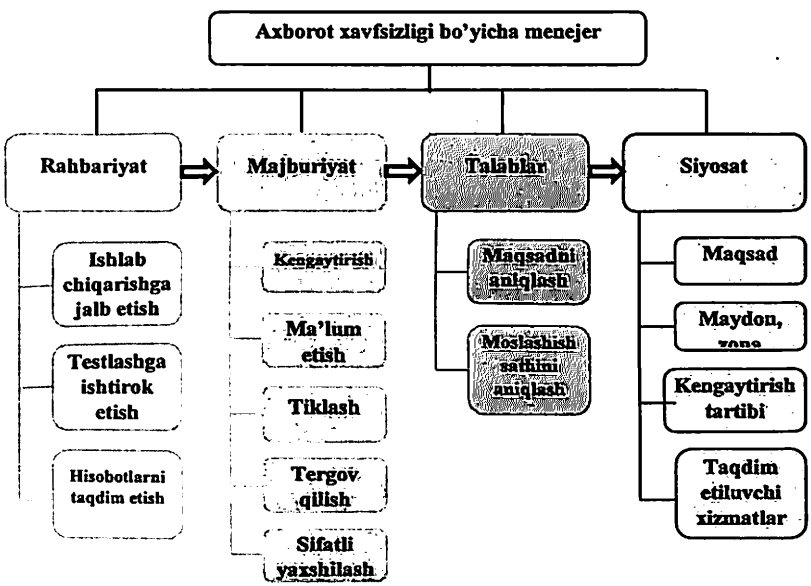
1.7-rasm. Axborot xavfsizligi insidentlarini olidini olishni hujjatlashtirish

Axborot xafsizligidagi kutilmagan holatlarni oldini olish prosedurasi

1. Insidentni tezkor aniqlash.
2. Insidentni aniq identifikasiyalash.
3. Insidentni to‘g‘ri boshqarish.
4. Insidentni to‘xtatish va kamaytirish.
5. Xizmatlarni tiklash.
6. Sababni tushunish.
7. Takrorlashni bartaraf etishda tadbiq qilishni yaxshilash.

Eng avvalo insidentlarni boshqarish jarayonlarini boshqaruvchi javobgar shaxsni aniqlab olish zarur. Ko‘p hollarda bu xafsizlik bo‘limi boshlig‘i bo‘ladi. 1.8-rasmda kutilamgan insidentlarni bartaraf etish bo‘yicha asosiy yechim harakatlari ketma ketligi ko‘rsatilgan.

Talablar va siyosatni ishlab chiqish - ekspert yechim, bu ishlab chiqaruvchining malakasi va tajribasiga, hamda biznes talablar va maqsadlarga bog‘liqdir.



1.8-rasm. Insidentlarni bartaraf etish bo‘ycha asosiy yechimlar

Rollarni taqsimlash - asosiy harakatlardan biri hisoblanadi, insidentlarni boshqarish jarayonlarini qurish tajribasiga asosan yo‘llarni tanlab, ular orasidan xato yo‘llarni ajratish orqali amalga oshiriladi.

Asosiy xulosalar

Axborot xavfsizligi insidenti – bu axborot xavfsizligi tizimidagi bir yoki bir necha tasodifiy va kutilmagan hodisalar, ish jarayonlarini tahlil qilishga katta imkoniyat berish va axborot himoyasini tahdidga qo'yilishi bilan bir qatorda axborot xavfsizligi tizimiga amalga oshiriladigan hodisalar, axborot xavfsizligiga kutilgan va kutilmagan tahdidlar yig'indisidir.

AX umumiy strategiyasining asosiy qismi sifatida tashkilot AX insidentlarini boshqarishga strukturalangan va aniq rejalashtirilgan yondashuvni ta'minlash maqsadida boshqaruv vositalari va taomillarni joriy etishi zarur. Tashkilotning nuqtai nazaridan, asosiy maqsad – AX insidentlariga yo'l qo'ymaslik yoki insidentlar tufayli o'z faoliyatiga yetkazilishi mumkin bo'lgan bevosita va bilvosita zararni imkon qadar kamaytirish uchun AX insidentlarining ta'sirini to'xtatib turish. Axborot resurslariga yetkaziladigan zarar faoliyatga salbiy ta'sir qilishi mumkin, shunday ekan operasion va biznes-jarayonlar to'g'risida tushuncha AXni boshqarishning muayyan maqsadlarini aniqlashga katta ta'sir qilishi lozim.

Insidentni boshqarish - biznes jarayonlarni olib borish jarayonida ish holatini tezda minimal xavf bilan normal ish holatiga qaytarish faoliyati hisoblanadi, hamda qisqa davom etadigan va bir maqsad sari yo'naltirilgan xizmatlar qatoriga kiradi.

Insidentni boshqarish bo'yicha asosiy standartlar quydagilar hisoblanadi.

- ISO/IEC 27001:2013;
- ISO/IEC TR 18044;
- CMU/SEI-2004-TR-015;
- NIST SP 800-61;
- GOST R ISO/MEK 18044;

Eng avvalo insidentlarni boshqarish jarayonlarini boshqaruvchi javobgar shaxsni aniqlab olish zarur. Ko'p hollarda bu xafsizlik bo'limi boshlig'i bo'ladi. Axborot xavfsizligi insidentlarini aniqlash, axborot xavfsizligi insidentlarini olidini olishni hujjatlashtirish, insidentlarni bartaraf etish bo'ycha asosiy yechimlar bo'yicha tegishli ko'rsatmalar keltirib o'tildi.

Nazorat uchun savollar

1. « Axborot xavfsizligi insidenti » iborasi nimani anglatadi?
2. Insidentni boshqarish prinsiplari.
3. Insidentga javob qaytarishni rejalashtirish va tayyorlash bo'yicha qo'llanma o'zichga qanday malumotlarni qamrab olgan?.
4. Axborot xavfsizligi insidentlarini boshqarishning maqsad va vazifalari.
5. Hodisalar va axborot xavfsizligi insidentlari tushunchasi.
6. Axborot xavfsizligi insidentlari bilan ishlash deganda nima tushunasiz.
7. Insedentlar haqida ma'lumot berishda qanday ma'lumotlar asosiy hisoblanadi.
8. Helpdesk nima ?
9. Foydalanuvchilardan kelgan to'g'ridan-to'g'ri xabarlar qanday xabarlar hisoblanadi ?
10. AX xodimlari tomonidan aniqlangan insidentlar boshqa insidentlardan nimasi bilan farq qiladi ?
11. Boshqarish funksiyasi va mohiyati.
12. AX insidentlarini boshqarish etaplari nechta ?
13. Axborot xafsizligidagi kutilmagan holatlarni oldini olish prosedurasi ketma ketligi qanday?
14. Rollarni taqsimlash nima ?

2. AXBOROT XAVFSIZLIGI INSIDENTLARINI BOSHQARISHDA NORMATIV BAZALAR

2.1. O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016): standartiga muvofiq axborot xavfsizligi insidentlarini boshqarish bosqichlari

O‘z DSt 3386, O‘z DSt 3387 standartlar O‘z DSt ISO/IEC 27000 standartlar seriyasining davomi bo‘lib, asosiy e’tiborni axborot xavfsizligi (AX) insidentlarini boshqarishga qaratadi. O‘z DSt ISO/IEC 27000 standartlar seriyasiga muvofiq, bunday boshqarish axborot xavfsizligini boshqarish tizimining (AXBT) muvaffaqiyatini ta’minlashda hal qiluvchi omillaridani biri deb belgilangan.

Tashkilotning AX insidentlarini boshqarish rejasi va tashkilotning insidentlarga javob qaytarishga tayyorligi to‘g‘risida xabardorligi o‘rtasida katta farq mavjud. Shuning uchun, ushbu standartda tashkilotning AX insidentiga javob qaytarishga haqiqatan tayyorligiga bo‘lgan ishonchini oshirish bo‘yicha rahbariy ko‘rsatmalarni ishlab chiqish ko‘rib chiqiladi. Bunga insidentlarni boshqarish bilan bog‘liq siyosatlar va rejalarni ko‘rib chiqish, AX insidentlariga javob qaytarish guruhini (AXIJQG) tashkil etish hamda uning ishini takomillashtirish orqali erishiladi.

Ushbu standartga ko‘ra, bayon etilgan maqsadlarga erishish uchun AX insidentlarini boshqarish quyidagi beshta alohida bosqichdan iborat:

- rejalashtirish va tayyorgarlik ko‘rish;
- aniqlash va hisobot;
- baho berish va qaror qabul qilish;
- javob choralari ko‘rish;
- ortirilgan tajriba.

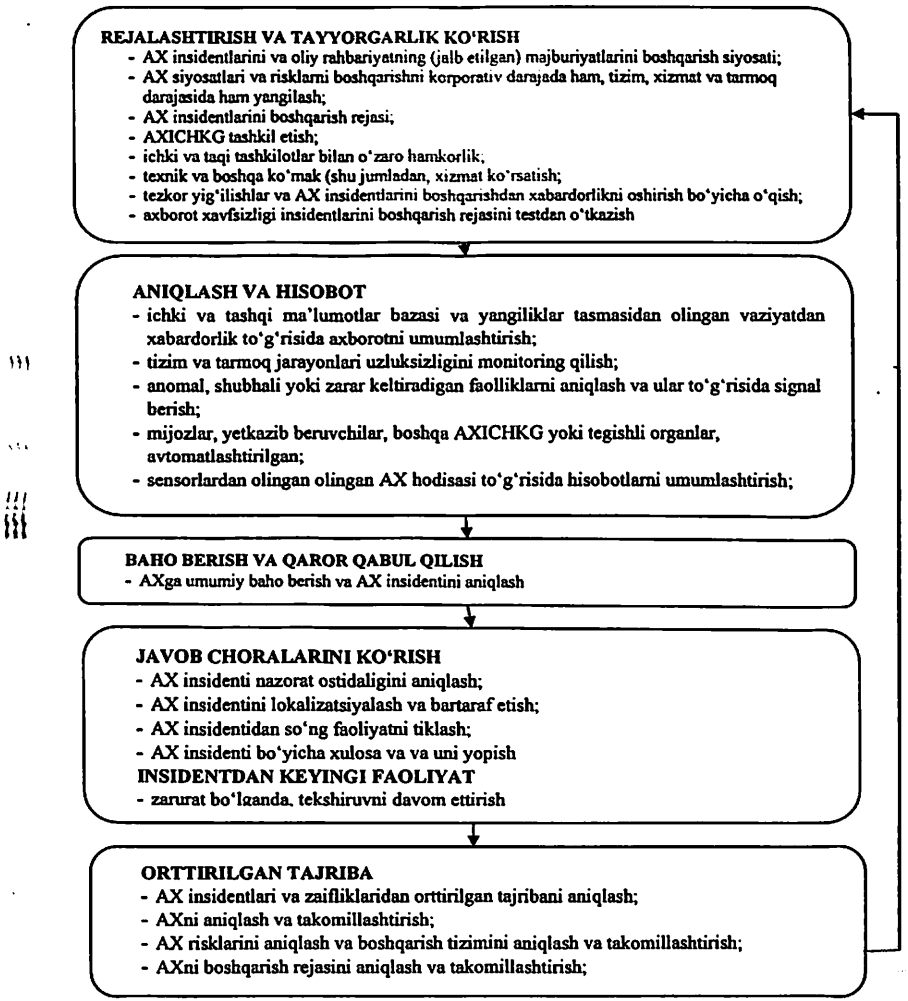
Mazkur bosqichlar 2.1-rasmda batafsil ko‘rsatilgan.

Ayrim ish-harakatlar insidentlar bilan ishlash jarayonining bir necha bosqichida yoki butun jarayon mobaynida sodir etilishi mumkin. Bundayfaoliyat turlariga quyidagi ish-harakatlar kiradi:

- hodisalar, insidentlar va muhim axborotni, ko‘rilgan choralar va insidentlar bilan ishlash jarayoni doirasidagi keyingi ish harakatlarni hujjatlashtirish;
- ishtirok etuvchi taraflarni muvofiqlashtirish va ular o‘rtasidagi aloqa;
- rahbariyat va boshqa manfaatdor taraflarni muhim insidentlardan xabardor qilish;

- manfatdor taraflar va yetkazib beruvchilar va boshqa axborot xavfsizligi insidentlariga chora ko‘rish guruhi kabi ichki va tashqi xodimlar o‘rtasida axborot almashish.

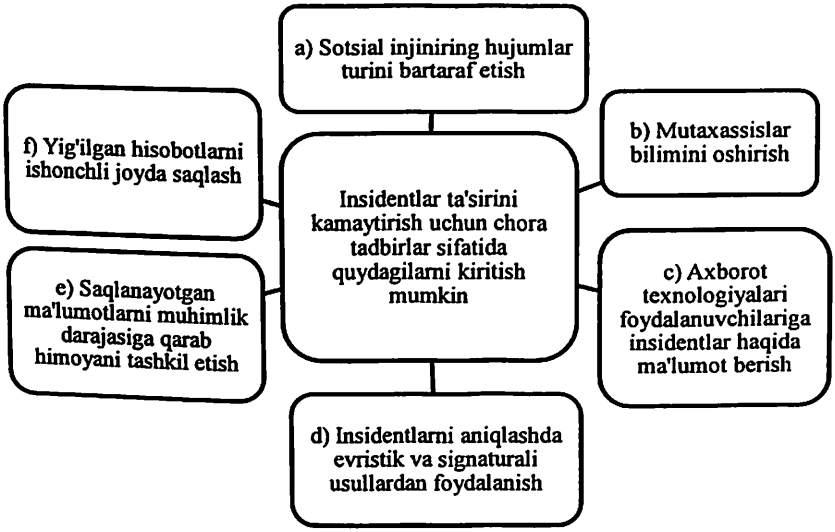
O‘z DSt 3386 standarti mavjud beshta bosqichni qamrab oladi. O‘z DSt 3387 standarti “Rejalashtirish va tayyorgarlik ko‘rish” va “Orttirilgan tajriba” bosqichlarini qamrab olgan. 2.2-rasmda AX insidentlarini boshqarish bosqichlarida AX insidentlari va hodisalari oqimi va ular bilan bog‘liq ish-harakatlar ko‘rsatilgan.



2.1-rasm. AX insidentlarini boshqarish bosqichlari

Insidentlar ta'sirini kamaytirish

Axborot xavfsizligi insidenntlarini ta'sirini kamaytirish uchun birinchi navbatda ularni kelib chiqish sabablari o'rganiladi.



2.2-rasm. Insidentlar ta'sirini kamaytirish

Ya'ni bu insidentlar qanday sodir bo'ldi, kim tomonidan, atayin qilindimi yoki tabiiy ofatmi, maqsadi aniqlanadi va to'liq hisobot yig'iladi. Mutaxassisdan yuqori darajadagi bilim va malaka talab etiladi.

2.2. Axborot xavfsizligi insidentlarini boshqarish siyosati

Axborot xavfsizligi insidentlari boshqarish siyosatini (AXIBS) shakllantirish muammolarini yechishda muhim vazifa AXI boshqarish muolajasi detalizasiyasi va AX insidentlari boshqaruvi formallashgan modelini qurish bilan bog'liq. AXI boshqaruv muolajasini izohlash uchun PCDA modeli – jarayonlarni uzluksiz yaxshilash klassik modelidan foydalaniladi. AXIBS ni formal namoyishi uchun quyidagi vazifa yechimlarini ko'rib chiquvchi kompleks yondashuv tanlangan:

- Axborot xavfsizligi insidentlari hisoblash, ma'lum qilish va aniqlash.
- Axborot xavfsizligi insidentlariga reaksiya, oldini olish uchun kerakli vositalar qo'llanilishi va yetkazilgan zararni tiklash va kamaytirish.

- Axborot xavfsizligini butunligicha ta'minlash jarayonini yaxshilash va oldini oluvchi himoya choralarini rejalashtirish maqsadida sodir bo'lgan insidentlarni tahlillash.

Formallashgan model nazariy-ko'plik va mantqiy shakllarda namoyish etiladi. Taklif etilayotgan AXIBS formallashgan modeli kompaniyaga yetkaziladigan zarar haqida ogohlantirmaydi, biroq uni tashkil etish orqali tashkilotning mavjud himoya tizimini samaradorligini oshirish va qayta zarar ko'rish ehtimolini kamaytirishga erishish mumkin.

Axborot xozirgi kunda tashkilotning raqobatbardoshligini ta'minlovchi asosiy resurslardan biri bo'lib, tashkilot himoya masalarini ham aktuallashtiradi. Axborotni himoyalash tizimidagi zaifliklar moliyaviy yo'qotishlarga, tijoriy operasiyalarga zarar yetkazishga va natijada kompaniyani "bozor uchun kurash"dan chiqarib yuborilishiga olib kelishi mumkin. Shunday ekan zamonaviy kompaniyalarning birinchi strategik vazifasi tizimda sodir bo'luvchi axborot xavfsizligi insidentlarini boshkarish imkoniyati mavjud axborotni samarali himoyalash tizimini yaratish hisoblanadi.

GOST R 18044-2007 "Axborot texnologiyalari. Xavfsizlikni ta'minlash vositalari va metodlari"ga asosan, "axborot xavfsizligi insidenti - AX tahdid yaratilishi va biznes-operasiyalar o'zaro kelishish ehtimoliy qiymati bilan bog'liq bir yoki bir necha kutilmagan AX hodisalarini paydo bo'lishidir".

Ularning natijasi axborotni fosh etilishi yoki o'zgartirilishi, o'chirilishi yoki axborotni foydalanmaydigan qilib qo'yuvchi boshqa hodisalar va tashkilot aktivlariga zarar yetkazilishi yoki o'g'irlanishi bo'lishi mumkin.

Insident sifatida aniqlangan, lekin bu haqda xabar qilinmagan AX insidentlarini o'rganib chiqish mumkin emas va bu insidentlarini oldini olish uchun himoya choralarini ko'rishning iloji yo'q.

Bunga qaramasdan tashkilotda AXI sodir bo'lganlik ehtimoli uch asosiy faktorga mos bo'lishi kerak:

- AXI haqidagi xabar bir vaqtning o'zida bir nechta manbalardan keladi (foydalanuvchilar, IDS, jurnal fayllari);
- IDS ko'plab qaytariluvchi hodisalar haqida signal beradi;
- Avtomatlashtirilgan tizimlar jurnal fayllar tahlili insident hodisasi bo'lish imkoniyati haqida tizim administratori xulosasi uchun asos bo'ladi.

GOST R 53114-2008 "Axborot himoyasi. Tashkilotda axborot xavfsizligini ta'minlash. Asosiy termin va atamalar"ga asosan tashkilotning axborot xavfsizligi boshqaruvi "qo'llanma bo'yicha koordinasiyalangan harakat va tashkilotning ichki va tashqi muhit o'zgaruvchi shartlariga mos AX ni tashkilotda ta'minlashni boshqarishdir". Joriy GOSTga asosan tashkilot axborot xavfsizligini boshqarish siyosati biznes, tashkilot, uning aktivlari va texnologiyalari xarakteristikasiga asosida aniqlanishi kerak:

- AX sohasidagi harakatlar asosiy prinsipi va yo'nalishi, maqsadlarini o'z ichiga oluvchi kosepsiyadan iborat;
- Xavfsizlikni ta'minlash bo'yicha shartli majburiyatlarni, ma'muriy-huquqiy talablarni hamda biznes talablarni e'tiborga oladi;
- AX boshqaruviga amal qiluvchi va bu bo'yicha ishlab chiqiluvchi tashkilot boshqaruv tahdidlari strategiyasiga rioya etadi;
- Tahdidlarni baholash kriteriyalarini o'rnatadi;
- Tashkilot rahbariyati tasdiqlaydi.

Bunda AXIBS ni samarali amalga oshirish uchun tashkilot monitoringi, qo'llash va uzluksiz hujjatlashtirish tizimini eksplutasiya qilish va funksional planda ta'minlanishi, tadbiq qilinishi, ishlab chiqilishi kerak.

Natijali AXIBS ga erishish uchun kerakli rejalashtirishdan so'ng ko'rilgan muolaja siyosatlarni, qator tayyorlangan harakatlarni va quyidagilarni o'z ichiga oluvchi harakatlarni bajarish kerak:

1. AX insidenti boshqarish siyosatini ishlab chiqish va shakllantirish, yana yuqori raxbariyatdan bu siyosat tasdig'ini olish;
2. AX insidentlar boshqarish tizimini batafsil hujjatlashtirish va ishlab chiqish. GOST R 18044-2007 «Axborot texnologiyalari. Xavfsizlikni ta'minlash vositalari va metodlari. Axborot xavfsizligi insidentlari boshqaruvi»ga binoan, AX insidentlari boshqarish tizimlarini hujjatlashtirish AX insidentlar klassifikasiyasi uchun jiddiylik shkalasi va hujjatlashtirilgan muolajalari va ma'lumotlar foydalanish muolajalarga havolalar bilan bog'liq harakatlarga mos va biznesni uzluksizligini ta'minlash plani, tarmoq zaxiralanishi va servislar tizimi AX insidentlari va hodisalari haqidagi hisobotlar shakllaridan iborat bo'lishi kerak;
3. kirish, chiqish yoki hujum qilinayotgan tizimda, servisda va (yoki) ma'lumotlar tarmog'ida joylashgan oqim monitoringi tadbiq qilish;

4. Ikkilanuvchi muolajani aktivlashtirish elementlari va tarmoq va (yoki) servis, tizim xavfsizlik siyosatiga binoan biznes uzluksiz rejalashtirishi bo'yicha harakatlar;

5. Monitoringni olib borish va tashkilot ichki tartibli taftishi yoki sud ishlari uchun ehtiyoj bo'lgan holatlarda dalillarni elektron shaklda himoyalangan holda saqlashni tashkil etish;

6. AX insidentlari haqida tafsilotlarni tashkilot xodimlariga va boshqa shaxslarga yoki tashkilotlarga yuborish;

7. AX insidentlari boshqarish tizimini, uning jarayonlarini va muolajalarini sinovdan o'tqazish;

8. Boshqaruv siyosatini yangilash va AX tahdidlar tahlili, AX korporativ siyosatlari, tizim, servislar uchun va (yoki) AX insidentlar boshqaruvida havolalar ishlashi uchun tarmoqlar AX maxsus siyosati va AX insidentlar boshqaruvi tizimi chiqish ma'lumotlari konteksida bu siyosatlarni davomiy ko'rib chiqishni ta'minlash;

9. AX insidentiga qarshi harakat guruhi (AXIQHG) personaliga mos dasturiy bilim o'rgatish;

10. AX insident boshqarish tizimini (va AXIQHG faoliyatini) texnik va boshqa vositalar bilan qo'llab-quvvatlash;

11. AX insidentlarini boshqarish haqida xabardorlikni ta'minlash dasturlarini loyihalash va ishlab chiqish, tashkilotning barcha personalini bu dastur bilan tanishtirish.

Tashkilotda AX boshqarish tizimi tashkilot joriy rivojlanish umumiy shartlarini shakllantiruvchi asosiy faktorlar, kompaniya faoliyati xarakterini hisobga olgan holda amalga oshiriluvchi, ichki va tashqi xavflarni oldini olishga yo'naltirilgan, aniq bir tashkilotda axborot xavfsizlik insidentlarini boshqarish siyosati kabi aniqlanuvchi tashkilot AXI boshqaruv siyosati shaklida namoyish etiladi.

2.3. Axborot xavfsizligi insidentlarini boshqarishning meyoriy asoslari

Axborot xavfsizligi insidentlarini boshqarishda ishlatiladigan standartlar uchun ISO/IEC 27035 standarti asos hisoblanadi. Unda AX insiyentlarini boshqarishning asosiy bosqichlari va asosiy tushunchalar, bu tushunchalarning insidentlarni aniqlash, ular bo'yicha hisobot tuzish, baholash va chora ko'rishga hamda orttirilgan tajribani qo'llashga strukturalangan yondashuvning prinsplari bilan bog'liqligi bayon etilgan.

Mazkur standartda bayon etilgan prinsplar umumiy xususiyatga ega bo‘lib, turi, hajmi yoki faoliyat turidan qat’iy nazar barcha tashkilotlar tomonidan qo‘llash uchun mo‘ljallangan. Tashkilotlar o‘z turi, hajmi va faoliyat turidan kelib chiqib mazkur standartda keltirilgan qo‘llanmaga o‘zgartirish, AX risklari bilan bog‘liq vaziyatga nisbatan tuzatish kiritishlari mumkin. Mazkur standartni, shuningdek, AX insidentlarini boshqarish xizmatlarini taqdim etadigan tashqi tashkilotlarga nisbatan ham qo‘llash mumkin.

Axborot xavfsizligi insidentlarini boshqarishda ishlatiladigan standartlar.

ISO/IEC 27035-1:2016 Axborot texnologiyalari. Xavfsizligni ta’minlash usullari. Axborot xavfsizligi tizimidagi tasodiflarni boshqarish - 1-Qism: Insidentni boshqarish prinsiplari.

Bu standart asosida ishlab chiqilgan milliy standart O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi insidentlarini boshqarish. 1-qism. Insidentlarni boshqarish tamoyillari

ISO/IEC 27035-2:2016 Axborot texnologiyalari. Xavfsizligni ta’minlash usullari. Axborot xavfsizligi tizimidagi tasodiflarni boshqarish - 2-Qism: Insidentga javob qaytarishni rejalashtirish va tayyorlash bo‘yicha qo‘llanma.

Bu standart asosida ishlab chiqilgan milliy standart O‘z DSt 3367:2019 (ISO/IEC 27035-2:2016, MOD) Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi insidentlarini boshqarish. 2-qism. Insidentlarga javob choralarini rejalashtirish va amalga oshirish bo‘yicha rahbariy ko‘rsatmalar.

Ushbu standartlar quyidagi standartlar bilan uzviy bog‘liq hisoblanadi. Bular:

O‘z DSt ISO/IEC 27000:2014 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Sharh va lug‘at.

O‘z DSt ISO/IEC 27001:2016 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Talablar.

O‘z DSt ISO/IEC 27002:2016 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarishning amaliy qoidalari.

O‘z DSt ISO/IEC 27005:2013 Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish. O‘z DSt ISO/IEC 27010:2015 Axborot texnologiyasi. Xavfsizlikni ta’minlash

usullari. Sohalararo va tashkilotlararo kommunikasiyalarda axborot xavfsizligini boshqarish bo'yicha qo'llanma.

O'z DSt ISO/IEC 27031:2016 Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot-kommunikasiya texnologiyalarining biznesning uzluksizligini ta'minlashga tayyorligi bo'yicha rahbar ko'rsatmalar.

O'z DSt ISO/IEC 27037:2017 Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Raqamli dalillarni identifikasiya qilish, to'plash, olish va saqlash bo'yicha rahbariy ko'rsatmalar.

O'z DSt ISO/IEC 27040:2018 Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Ma'lumotlarni saqlash xavfsizligi.

O'z DSt 3361:2019 (ISO/IEC 27041:2015, MOD) Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Insidentlarni tekshirish usullari yaroqliligi va to'g'riligini ta'minlash bo'yicha qo'llanma.

2.4 Axborot xavfsizligi insidentlarini boshqarishni rejalashtirish va tayyorgarlik ko'rish

AX insidentlarini samarali boshqarish lozim tarzda rejalashtirish va tayyorgarlik ko'rishni taqozo etadi. AX insidentlarini boshqarish uchun amaliy va samarali reja qabul qilish uchun tashkilot quyidagi bir qator tayyorgarlik choralarini yakunlashi zarur:

1. oliy rahbariyatni jalb qilgan holda, AX insidentlarini boshqarish siyosatini ifodalash va ishlab chiqish;
2. AX siyosatlarini, shu jumladan boshqaruv risklari bilan bog'liq
3. siyosatlarni ham korporativ darajada, ham tizim, xizmat va tarmoqlarga nisbatan yangilash;
4. AX insidentlarini boshqarish muvaffal rejasini aniqlash va hujjatlashtirish, shu jumladan aloqa va axborotni oshkor etish masalalari;
5. ishlab chiqilgan va tashkilot xodimlariga taqdim etilgan tegishli o'quv dasturiga ega axborot xavfsizligi insidentlariga chora ko'rish guruhi tashkil etish;
6. AX hodisalari, insidentlari va zaifliklarini boshqarishga bevosita jalb etilgan ichki va tashqi tashkilotlar bilan tegishli munosabat va aloqa o'rnatish va qo'llab-quvvatlash;
7. AX insidentlarini va axborot xavfsizligi insidentlariga chora ko'rish guruhi faoliyatini boshqarish rejasini qo'llab-quvvatlash uchun texnik, tashkiliy va operasion mexanizmlarni yaratish, joriy etish va

foydalanish. axborot xavfsizligi insidentlariga chora ko'rish guruhini qo'llab quvatlash uchun zarur axborot tizimlarini, shu jumladan AX ma'lumotlar bazasini ishlab chiqish va amalga joriy etish. Ushbu mexanizm va tizimlar AX insidentlari kelib chiqishining oldini olish yoki kelish chiqishi ehtimolini kamaytirish uchun mo'ljallangan;

8. AX hodisalari, insidentlari va zaifliklarini boshqarish borasida o'quv va xabardorlikni oshirish dasturini ishlab chiqish;

9. AX insidentlari, jarayonlari va taomillarini boshqarish rejasidan qanday foydalanilayotganini tekshirish.

Ushbu bosqich yakunlanganidan so'ng tashkilot AX insidentlarini lozim tarzda boshqarishga to'liq tayyorlangan bo'lishi shart.

2.5. Axborot xavfsizligi insidentlarini identifikasiyalash va baholash mezonlari

Axborot xavfsizligi siyosatlari yoki boshqaruv vositalari o'z-o'zidan axborot, axborot tizimlari, xizmatlar yoki tarmoqlarning to'liq himoyasini kafolatlamaydi. Boshqaruv vositalari joriy qilingandan so'ng qolgan zaif nuqtalar axborot xavfsizligining samaradorligini kamaytirishi va natijada axborot xavfsizligi insidentlarini vujudga keltirishi extimoli mavjud. Potensial ravishda bu xolat tashkilotning faoliyatiga bevosita va bilvosita salbiy ta'sir ko'rsatishi mumkin. Bundan tashqari oldindan ma'lum bo'lmagan yangi xavf-xatarlar albatta vujudga keladi. Tashkiloting bunday insidentlarga qarshi kurashish uchun yetarli tajribasining yo'qligi har qanday javobning samaradorligini pasaytiradi va tashkilot faoliyatiga salbiy ta'sir ko'rsatadi.

Axborot xafsizligi insidentlari oldindan rejalashtirilgan yoki tasodifiy bo'lishi (masalan, xato yoki tabiiy ofat tufayli yuzaga kelgan) bo'lishi hamda texnik yoki fizik omillar ta'sirida ro'y berishi mumkin. Ularning natijasi ma'lumotni ruxsatsiz oshkor qilish, o'zgartirish, yo'q qilish yoki ma'lumotni ishlatib bo'lmaydigan holatga keltirish, tashkilot aktivlariga ziyon yetkazish yoki ularni talon-taroj qilish bo'lishi mumkin.

Axborot xavsizligini texnik insidentlari(anomal tarmoq faolligi, xizmatning ishdan chiqishiga mo'ljallangan hujumlar, ruxsat etilmagan ma'lumotni qo'lga kiritishga urinish, zararli kodni yuklash va hakozo) avtomatik aniqlanishi mumkin, masalan, nazorat yozuvlari tahlili qurilmalari, tarmoqlararo ekranlar, hujumlarni aniqlash tizimlari, zararli

kodlarni aniqlashning instrumental vositalari (antiviruslar) tomonidan yuboriladigan ogohlantirish signallari bo'lishi mumkin.

Bugungi kunga tashkilotlarni axborot tizimisiz tasavvur qilish qiyin. Bu esa o'z navbatida tashkilotdagi aktivlarni butunligini, maxfiyligini va haqiqiy ekanligini ta'minlash zarurligini bildiradi va natijada axborot xavfsizligini boshqaruv tizimini (AXBT) tashkil etishni belgilaydi. AXBT ni mustahkam xavfsilik asoslarini belgilaydi, axborot texnologiyalari resurslaridan tizimli tarzda foydalanishni tartibga soladi. Lekin AXBT dagi texnik o'zgarishlar ham resurlardan foydalanish uchun qulay muhitni yaratmaydi. Qulay muhitni yaratish inson faoliyati bilan uzviy bog'liqdur.

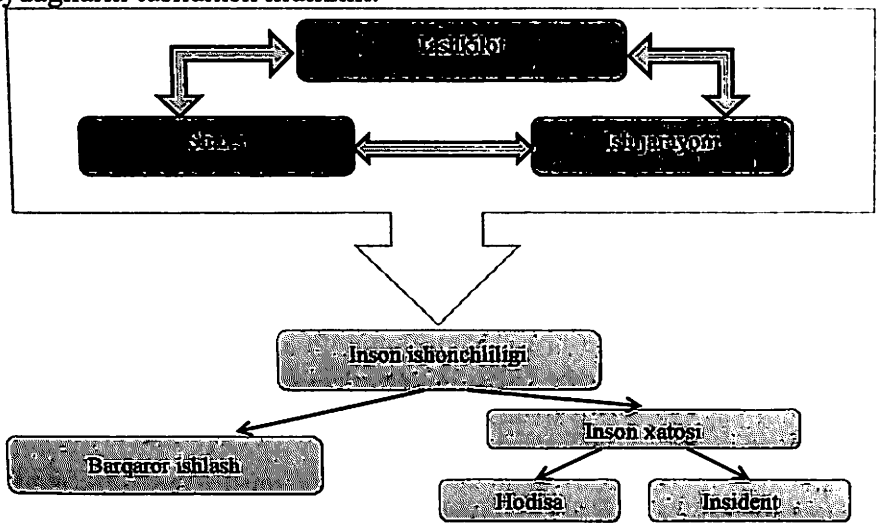
Axborot xavsizligida inson omili muhim rol o'ynaydi. Bugungi kunga kelib insidentlarni turli ko'rinishlarda uchratish mumkin. Insidentlarni yuzaga kelish sabablari ham turlicha. Aksariyat insidentlar inson omili natijasida yuzaga keladi. Bunga asosiy sabab sifatida axborot texnologiyalaridan foydalanuvchilarni yetarli darajada bilimga ega emalisliklari va sosial injineriyaninig juda yuqori suratlarda rivojlanishi axborot xavfsizligida yuqori darajadagi insidentlarni keltirib chiqardi.

Ko'plab axborot texnologiyalari tashkilotlari insidentlarga javob choralari hamda malakali xodimlarga ega bo'lsada bu tashkilotlar axborot xavfsizligi insidentlarini boshqarishlari murakkab jarayon hisoblanadi. Birinchi vazifa malakali mutaxassislarga ega bo'lish, ikkinchisi esa insidentlarga qarshi chora tadbirlarni ishlab chiqish hisoblanadi. Tashkilotning barcha resurslaridan foydalangan holda insidentlarni aniqlash va insidentlar haqida hisobot tayyorlash, boshqarish uchun omil hisoblanadi. Insidentlarni aniqlashni avtomatlashtirilgan tizimlarini hosil qilish va shu bilan birga real vaqtda javob choralarini ko'rishni tashkillashtirishni amalga oshirilishi lozim. Yangi axborot tizimlarida xavfsizlik insidentlarini avtomatik aniqlash tizmini rivojlantirishi uchun, tez-tez profilaktika ishlarini amalga oshirilish maqsadaga muvofiq.

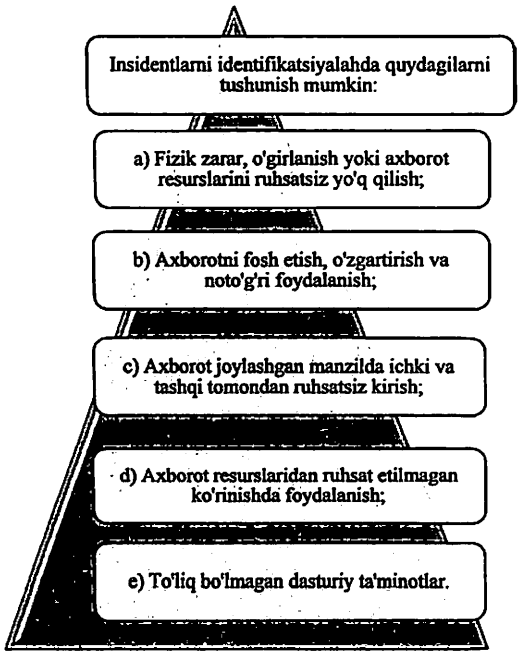
Axborot xavfsizligi insidentlarini identifikasiyalash va baholash mezonlari.

Axborot xavfsizligi insidentlarini identifikasiyalovchi tashkilotlar mavjud bo'lib ular qo'shimcha choralar, tegishli tuzatishlar va zarur bo'lsa takrorlanish extimolini kamaytirish tartiblarini ko'rib chiqadi. Korparativ Axborot Xavfsizligi Idorasi (CISO) KAXI mana shunday

ishlarni amalga oshiradi. Insidentlarni identifikasiyalash deganda quydagilarni tushunish mumkin:



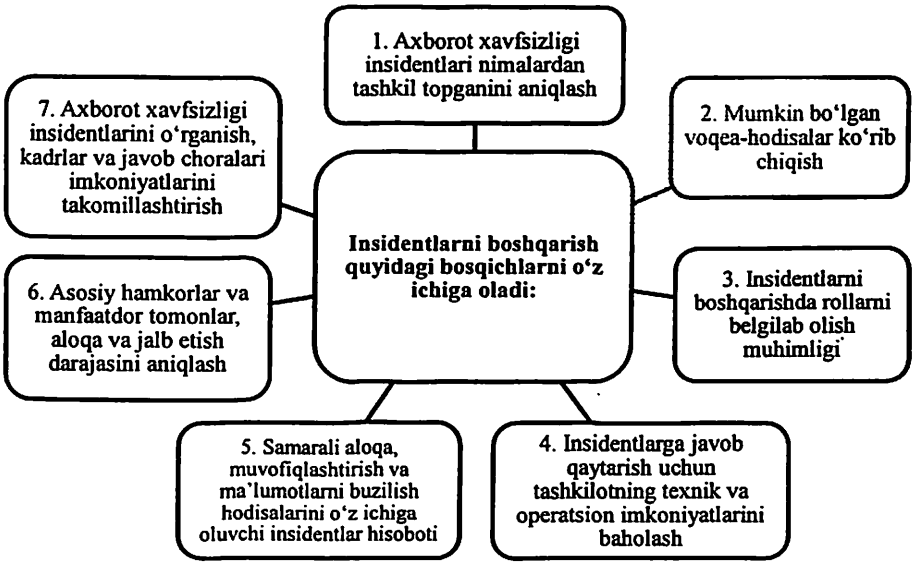
2.3-rasm. Insident faktorlarida inson omili



2.4-rasm. Axborot xavfsizligi insidentlarini identifikasiyalash jarayoni

Insidentlarini baholash va qaror qabul qilish mezonlari.

Axborot xavfsizligida ma'lumotlarni himoya qilish ko'lami juda keng. Shu sababli vaqti-vaqti bilan baholashlarni amalga oshirish, insidentlarni boshqarish qobilyatlarini takomillashtirish muhim ahamiyat kasb etadi. Insidentlarni boshqarish quyidagi bosqichlarni o'z ichiga oladi:



2.5-rasm. Insidentlarini baholash va qaror qabul qilish mezonlari

Baholash va qaror qabul qilish bosqichi uchun tashkilotlar quydagi chora-tadbirlarni ta'minlashi lozim:

1. Xodisa axborot xavfsizligi insidenti sifatida yoki yolg'on sifatida qabul qilinishi, agar yolg'on bo'lmasa bosqichma-bosqich keng o'rganilishi lozim;

2. hodisaning axborot xavfsizligi insidenti sifatida tasniflanishini aniqlash maqsadida axborot xavfsizligi insidentlariga qarshi kurash xizmati (AXIQKX) tomonidan baxo berilishidir. Axborot xavfsizligi insidenti qanday, kim tomonidan va qaysi ketma-ketlikda qayta ishlashi haqida qaror qabul qilinishi lozim. Bunda tahlil har bir axborot xavfsiligi insidentining tegishli turga mansub ekanligining ta'minlash uchun o'z ichiga oldindan belgilangan ketma-ketliklar

bo'yicha taqsimlash jarayonini o'z ichiga olishi va axborot xavfsizligi insidentlarini qayta ishlash va ularga javob qaytarish lozimligini aniqlash hamda tezkor javob choralarini ko'rishi lozim;

3. ma'lumotlarni elektron shaklda yig'ish va xafvsiz saqlanishini hamda ichki intizomiy choralarni doimiy nazoratini ta'minlash.

Axborot xavfsizligi insidentlari yoki zaifliklari bo'yicha barcha yig'ilgan ma'lumotlar AXIQKX raxbarligidagi axborot xavfsizligi insidentlari ma'lumotlar omborida saqalanishi kerak. Xar bir faoliyat turi jarayonida xabar beriladigan barcha ma'lumotlar baxo berish va qaror qabul qilish va tegishli choralar ko'rish uchun foydalanilgan omborni ta'minlash uchun to'liq bo'lishi lozim.

Axborot xavfsiligi hodisasi axborot xavfsizligi insidenti sifatida aniqlangan bo'lsa baxo berishning keyingi bosqichiga o'tkaziladi. Buning natijasida tuzatish harakatlari, masalan, qo'shimcha avariyaviy himoya choralarini aniqlash, boshqa mutaxassislardan maslahat so'ralishi mumkin:

a) Axborot xavfsizligi insidenti nimadan iborat ekanligi.

b) Uning sababi kim yoki nima ekanligi.

c) U nimaga ta'sir qilishi va qilishi mumkinligi.

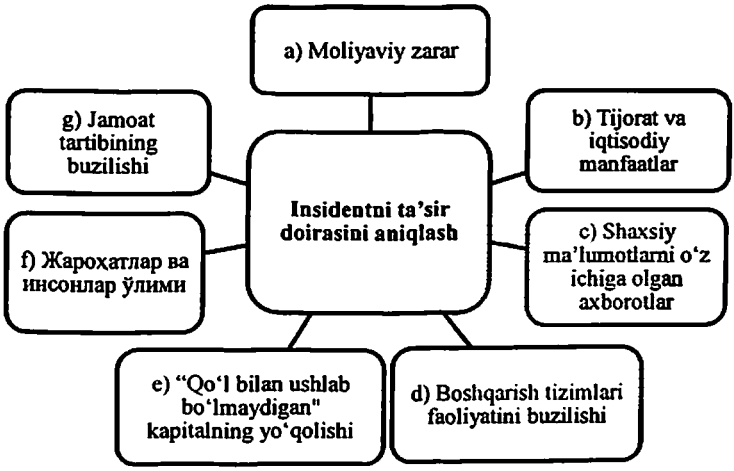
d) Axborot xavfsizligi insidenti tashkilot biznesiga real yoki extimoliy ta'siri.

e) Axborot xavfsizligi insidentining muhimlilik darajasi.

f) Axborot xavfsizligi insidenti bungacha qanday qayta ishlanganligi.

Birinchi bo'lib quyidagi oqibatlardan qaysi biri ahamiyatli ekanligi aniqlanadi (2.7-rasm).

Jarayonlar ko'lamining kengayishi insidentlarning muhim elementi hisoblanadi. Qizig'i shundaki insidentlar tashkilotning faoliyatidan kelib chiqqan holda turlicha bo'ladi. Insidentlar muayyan sharoitda faol tizimlarni va tarmoqlarning monitoringini o'tkazish siyosatini qilinadi. Bundan tashqari ma'lumotlarni auditlash va kimdir shu ma'lumotlarga kirmoqchi bo'lsa maxsus ruxsatnomaga ega bo'lishi talab qilinadi. Tekshirish davomida sodir bo'lmagan insidentlar haqidagi ma'lumotlarni ko'rib chiqish lozim bo'ladi.



2.7-rasm. Insidentlarni ta'sir doirasini aniqlash

AX insidentlarini boshqarishning uchinchi bosqichi AX hodisalari bilan bog'liq axborotni baholashni va hodisani AX insidenti sifatida baholash kerak-kerakmasligi haqida qaror qabul qilishni o'z ichiga oladi. AX hodisasi aniqlanganidan va hisobot tuzilganidan so'ng, "Baho berish va qaror qabul qilish" bosqichida tashkilot quyidagi asosiy faoliyatlarni amalga oshirish zarur:

1. xodimlarning tegishli iyerarxiyasi yordamida, ham xavfsizlik xizmati xodimlarini, ham boshqa xodimlarni jalb qilgan holda, AX insidentlarini yaxshilash, shu jumladan, baho berish, qaror qabul qilish va ish-harakatlarni amalga oshirish bo'yicha tadbirlar uchun javobgarlikni taqsimlash;

2. xabardor qilingan har bir shaxsga amal etilishi majburiy bo'lgan taomillarni taqdim etish, shu jumladan tuzilgan hisobotlarni ko'rib chiqish va o'zgartirish, yetkazilgan zararni baholash va tegishli xodimlarni xabardor qilish. Individual ish-harakatlar insidentning turi va jiddiyligiga bog'liq bo'ladi;

3. agar AX hodisasi AX insidenti sifatida tasniflanadigan bo'lsa,

4. rahbar prinsplardan AX hodisalarini va AX insidenti uchun keyingi ish-harakatlarni batafsil hujjatlashtirish uchun foydalanish;

5. test, o'lchov ma'lumotlari va AX hodisasini aniqlashga doir boshqa

6. ma'lumotlarni o'z ichiga olishi mumkin bo'lgan axborotni umumlashtirish. To'plangan axborot turi va miqdori sodir bo'lgan AX hodisasiga bog'liq;

7. hodisa potensial yoki tasdiqlangan AX insidentimi yoki yolg'on trevoga signalimi, bilish uchun, insidentlar ustida ishlovchi tomonidan baholash o'tkazilishi. Yolg'on trevoga signali (ya'ni, xato ruxsat berilishi) hisobotda haqiqatan emas yoki hech qanday oqibatlarga ega emas deb ko'rsatilgan hodisa sodir bo'lganidan dalolat beradi. axborot xavfsizligi insidentlariga chora ko'rish guruhi, insidentlar ustida ishlovchi insidentni to'g'ri baholaganiga ishonch hosil qilish uchun, sifat tekshiruvini o'tkazishi mumkin;

8. barcha jalb etilganlar, ayniqsa axborot xavfsizligi insidentlariga chora ko'rish guruhi tomonidan barcha ish - harakatlari tegishli qabul qilingan qarorlar keyinchalik tahlil qilish uchun lozim tarzda qayd etilishi ta'minlanishi;

9. AX hodisalari va zaifliklarini topish va ular bo'yicha hisobot tuzish funksiyalarini yangilash imkonini beradigan o'zgarishlarni nazorat qilish rejimiga amal qilish, shuningdek AX ma'lumotlar bazasini dolzarb holatda saqlash.

AX hodisasi yoki zaifligiga talluqli bo'lgan barcha to'plangan va umumlashtirilgan axborot axborot xavfsizligi insidentlariga chora ko'rish guruhi tomonidan boshqariladigan AX ma'lumotlar bazasida saqlanishi lozim. Har bir tadbir davomida hisobotda ko'rsatilgan axborot ayni paytda imkon qadar to'liq bo'lishi shart, bu unga tegishli baho berilishiga, tegishli qaror qabul qilinishi va ish-harakatlar amalga oshirilishiga olib keladi.

Asosiy xulosalar

Tashkilotning AX insidentlarini boshqarish rejasi va tashkilotning insidentlarga javob qaytarishga tayyorligi to'g'risida xabardorligi o'rtasida katta farq mavjud. Shuning uchun, tashkilotning AX insidentiga javob qaytarishga haqiqatan tayyorligiga bo'lgan ishonchini oshirish bo'yicha rahbariy ko'rsatmalarni ishlab chiqish kerak.

Axborot xavfsizligi insidenntlarini ta'sirini kamaytirish uchun birinchi navbatda ularni kelib chiqish sabablari o'rganiladi. Axborot xavfsizligi insidentlari boshqarish siyosatini shakllantirish muammolarini yechishda muhim vazifa AXI boshqarish muolajasi detalizasiyasi va AX insidentlari boshqaruvi formallashgan modelini qurish bilan bog'liq. AXI boshqaruv muolajasini izohlash uchun PCDA modeli – jarayonlarni uzluksiz yaxshilash klassik modelidan foydalaniladi. Axborot xavfsizligi insidentlarini identifikasiyalovchi tashkilotlar mavjud bo'lib ular qo'shimcha choralar, tegishli tuzatishlar va zarur bo'lsa takrorlanish extimolini kamaytirish tartiblarini ko'rib chiqadi. Korparativ Axborot Xavfsizligi Idorasi (CISO) KAXI mana shunday ishlarni amalga oshiradi.

Axborot xavfsizligi insidentlari yoki zaifliklari bo'yicha barcha yig'ilgan ma'lumotlar AXIQKX raxbarligidagi axborot xavfsizligi insidentlari ma'lumotlar omborida saqalanishi kerak. Xar bir faoliyat turi jarayonida xabar beriladigan barcha ma'lumotlar baxo berish va qaror qabul qilish va tegishli choralar ko'rish uchun foydalanilgan omborni ta'minlash uchun to'liq bo'lishi lozim.

AX insidentlarini boshqarishning uchinchi bosqichi AX hodisalari bilan bog'liq axborotni baholashni va hodisani AX insidenti sifatida baholash kerak-kerakmasligi haqida qaror qabul qilishni o'z ichiga oladi.

Nazorat uchun savollar

1. Axborot xavfsizligi insidentlarini boshqarish bosqichlari sanab bering.
2. Axborot xavfsizligi insidentlari boshqarish siyosati tushuntiring.
3. Axborot xavfsizligi insidentlari sodir bo'lganlik ehtimoli nechta asosiy faktorga mos bo'lishi kerak.
4. Axborot xavfsizligi insidentlarini boshqarishning meyoriy asoslari tushuntirib bering.
5. Insident faktorlarida inson omili deganda nima tushunasiz.
6. Axborot xavfsizligi insidentlarini identifikasiyalash deganda nima tushunasiz?

3. AXBOROT XAVFSIZLIGI INSIDENTLARI VA HODISALARI TO‘G‘RISIDAGI HISOBOT

3.1. Axborot xavfsizligi insidentlari va hodisalari to‘g‘risidagi hisobot

AX insidentlarini boshqarishning asosiy bosqichlaridan biri AX hodisalarini aniqlashni, ular bilan bog‘liq axborotni umumlashtirishni va ularning yuzaga kelishi va zaifliklar mavjudligi yuzasidan qo‘l yoki avtomatlashtirilgan vositalar yordamida tayyorlangan hisobotlarni o‘z ichiga oladi. Bu bosqichda hodisalar va zaifliklar xali axborot xavfsizligi insidenti sifatida tasniflanmasligi mumkin.

AX hodisalari to‘g‘risida hisobot tashkilotning hisobotlar to‘g‘risidagi siyosatiga muvofiq, zarurat bo‘lganda, izchil tahlil qilishimkonini beradi.

AX hodisalarini aniqlash va hisobot tuzish bosqichida tashkilot quyidagi asosiy ish-harakatlarni amalga oshirishi zarur:

1. Bosh tashkilot va uning tarkibidagi tashkilotlarning tizim va tarmoqlaridagi faolliklarni monitoring va qayd qilish (bayonnoma tuzish);
2. AH hodisasini aniqlash, u aniqlanganligi yoki AX zaifligi borligi to‘g‘risida xodimlar tomonidan ham qo‘lda, ham avtomatlashtirilgan tarzda hisobot tayyorlash;
3. AX hodisalari yoki zaifligi to‘g‘risida axborotni umumlashtirish;
4. Ichki va tashqi ma’lumotlar bazasidagi, shu jumladan tizim va tarmoqdagi faolliklarni qayd etish jurnallaridagi AX bo‘yicha chora-tadbirlarga ta’sir qiladigan axborotni, joriy siyosiy, ijtimoiy yoki iqtisodiy faoliyat, insidentlarga taalluqli tendensiyalar, yangi hujum yo‘nalishlari, hujumlarning oqibatlarini yumshatish bo‘yicha yangi strategiyalar va texnologiyalar to‘g‘risidagi axborotni umumlashtirish;
5. Kelgusida tahlil qilish uchun barcha ish-harakatlar, natijalar va qabul qilingan tegishli qarorlar lozim tarzda qayd etilishini ta’minlash;
6. Sud surishtiruvi yoki ichki intizomiy tekshiruvlar uchun dalillar kerak bo‘lgan taqdirda, raqamli dallilar xavfsiz to‘planishi va saqlanishini, bunday xavfsiz saqlash uzluksiz monitoring qilinishini ta’minlash;
7. AX hodisalari va zaifliklarini topish va ular bo‘yicha hisobot tuzish funksiyalarini yangilash imkonini beradigan o‘zgarishlarni

nazorat qilish rejimiga amal qilish, shuningdek AX ma'lumotlar bazasini dolzarb holatda saqlash;

8. Zaruriyatga qarab, butun bosqich davomida tekshiruvlar yoki qabul qilingan qarorlar sonini ko'paytirish imkonini beradi.

AX hodisasi yoki zaifligiga talluqli bo'lgan barcha to'plangan va umumlashtirilgan axborot axborot xavfsizligi insidentlariga chora ko'rish guruhi tomonidan boshqariladigan AX ma'lumotlar bazasida saqlanishi lozim. Har bir tadbir davomida hisobotda ko'rsatilgan axborot ayni paytda imkon qadar to'liq bo'lishi shart, bu unga tegishli baho berilishiga, tegishli qaror qabul qilinishi va ish-harakatlar amalga oshirilishiga olib keladi.

3.2. Axborot xavfsizligi insidentlari va hodisalari qayta ishlash

Axborot texnologiyalarining tadbiq etilishi tashkilot va muassasalarda ish olib borish uslublari o'zgardi. Axborot texnologiyalari olib kirgan o'zgarishlar natijasida funksional jarayonlarni avtomatlashtirishga erishildi. Lekin axborot texnologiyalaridan foydalanish ilgari ma'lum bo'lmagan xavflarni keltirib chiqardi. Yuqori texnologiyalarning sohaga tadbiqi natijasida har qanday turdagi korxona faoliyatiga kiberjinoyatchilarning aralashishiga imkon tug'ildi.

Korxona ishiga bu tarzda aralashishning bir necha sabablari bor, odatda buzg'unchilar pullarni o'g'irlashga harakat qiladilar, lekin ba'zi hollarda esa ular korxona obrosiga putur yetkazish maqsadida yoki maxfiy ma'lumotni o'g'irlash uchun bu ishni amalga oshiradilar.

Axborot xavfsizligiga raxna soluvchi turli insidentlar mavjud. Eng ko'p tarqalganlari bu: DDoS-hujumlar ("xizmat ko'rsatishadan voz kechishga undaydigan hujumlar"), masofadan bank xizmatlaridagi firibgarlik (MBX), serverlarni buzish va konfidensial ma'lumotlarni o'g'irlash, korporativ ma'lumotlarni o'g'irlanishi, Internet tarmog'ida korxona obro'siga putur yetkazuvchi mish-mishlarni joylashtirish. Yuqorida sanalgan har bir insident talofat ko'rgan korxonalar obro'siga zarar yetkazadi.

Hozirgi kunda korxonalarda tashqi va ichki xarakterga ega bo'lgan axborot xavfsizligi insidentlari sodir bo'lmoqda.

Ichki insident – zarar ko'rgan tomon bilan bevosita (mehnat shartnomasi) bog'liq bo'lgan shaxs tomonidan amalga oshirilgan insident. Tizimda sodir bo'lishi mumkin bo'lgan quyidagi tez-tez uchrab turadigan holatlarni keltirish mumkin:

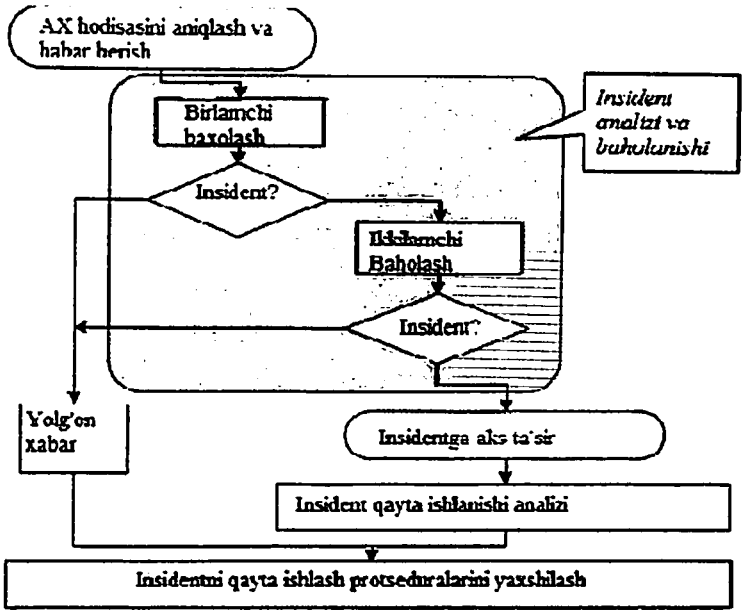
- konfidensial ma'lumotlarni o'g'irlanishi;
- axborotga ruxsat etilmagan kirish;
- ma'lumotlarni o'chirish;
- korxona aktivlarini shaxsiy maqsadlarda yoki firibgarlik uchun foydalanish;
- qo'poruvchilik;
- tarmoqdagi g'ayritabiy faollik;
- g'ayritabiy biznes shartnomalar;
- axborot texnologiyalari yordamida firibgarlik.

Tashqi insident – bu zarar ko'rgan tomon bilan hech qanday bog'liqligi bo'lmagan shaxslar tomonidan uyushtirilgan insident. Tizimda sodir bo'lishi mumkin bo'lgan quyidagi tez-tez uchrab turadigan holatlarni keltirish mumkin:

- MBX tizimlaridagi firibgarlik;
- DDoS hujumlar;
- trafikni qo'lga olinishi va almashtirib qo'yilishi;
- korxona brendidan Internetda noto'g'ri foydalanish;
- Fishing;
- korxonaning konfedensial ma'lumotlarini Internet tarmog'iga joylanishi;
- buzib kirish, buzib kirishga urinish, korxona portalini skanerlash;
- tarmoqni skanerlash, tarmoq tugunlarini skanerlashga urinish;
- virus hujumlari;
- konfedensial ma'lumotlarga ruxsat etilmagan kirish;
- g'ayritabiiy xatlar (tajovuzkor xatlar).

Hodisalarni qayta ishlash

Axborot tenologiyalari va kompyuter tarmoqlarining rivojlangan sari axborot xavfsizligi insidentlari soni ham oshmoqda, ular AX tizimi faolligiga raxna solib ko'ngilsiz holatlarga olib kelishi mumkin. Bularga misol qilib, konfidensiallikni buzilishini, axborot aktivlarining yaxlitligini buzilishi va biznes jarayonlarning uzilib qolishini keltirish mumkin. Axborot xavfsizligi insidentlarini qayta ishlashini boshqarish 3.1-rasmda keltirilgan.



3.1- rasm. Axborot xavfsizligi insidentlarini qayta ishlashini boshqarish

Xalqaro ISO 27001:2005 standarti axborot xavfsizligi insidentlarini boshqarish prosedurasini yaratishga alohida urg'u beradi – ma'lumki, sodir bo'lishi mumkin bo'lgan insidentlarning oldini olish, insidentlardan keyingi keladigan talofotlarni tuzatishdan ko'ra ancha samarali hisoblanadi. Xalqaro ISO/IEC 2705 va milliy GOST R ISO/MEK 18044:2007 standartlarda insidentlarni boshqarish jarayonlari keltirib o'tiladi. Normativ huquqiy hujjatlar va resurslar haqidagi savollar ko'riladi, bu jarayonlarni amalga oshirish bo'yicha tushuntirish va tavsiyalar berilgan.

3.3. Axborot xavfsizligi insidentlarini guruhlarga ajratish

Butun jaxon tajribasidan kelib chiqqan holda axborot xafsizligi insidentlarini xodimlar ishtiroki bilan quyidagi turlarga bo'lishimiz mumkin:

1. Ishchi ma'lumotlarni oshkor qilish.
2. Hisobotlarni soxtalashtirish.
3. Moliyaviy yoki material aktivlar o'g'irlanishi.
4. Korxona ishiga qarshi borish (sabotaj).
5. Lavozimni suiste'mol qilish.
6. Qoida buzarlikni yashirish.

Ishchi ma'lumotlarni oshkor qilish deganda korxona yoki ushbu ma'lumot chiqib ketmasligi zarur bo'lgan hudud doirasidan axborotni chiqarish nazarda tutiladi.

Ma'lumotlarni oshkor qilishni quyidagi usullarini sanab o'tish mumkin.

1. Ma'lumotni olish, bunday ma'lumotlar kirishi mumkin bo'lmagan hududlarda yoki katta massiv ma'lumotlar orasidan ajratib olishga aytiladi (malasan ma'lumotlar bazasidan ko'p hujjatlarni olish) bunda qoida buzuvchi ma'lumotni korxonada belgilangan hududdan tashqariga nusxalarda (hujjatlarning o'z foto nusxasi va h.k) yoki elektron ko'rinishda (flesh-xotirada va h.k) yoki ularni simsiz aloqa yo'li bilan uzatishi ham mumkin.

2. Ma'lumotlarni oshkor qilish, bunda insayder uchinchi shaxsga maslahat berishi mumkin. Bunday ma'lumot uzatish so'zlar bilan gaplashib amalga oshirilishi mumkin yoki insayder tomonidan tayyorlangan hujjatlardan kelib chiqqan holda olib boriladi.

Insayder tomonidan ishchi ma'lumotlarni olinishi mumkin bo'lgan usullar quyidagilar bo'lishi mumkin:

1. Insayder ma'lumotlarni maxsus tarzda qidirmaydi. Unga bu ma'lumotlar kutilmagan tarzda qo'lga tushib qolish sababi oshkor qilinadi, yoki bo'lmasa ushbu ma'lumotlar uning ish faoliyati uchun zarur ma'lumotlar bo'lishi mumkin.

2. Insayder ishchi ma'lumotlarga ruxsatnomasi bor va u o'ziga kerakli bo'lgan ma'lumotlarni qidirishi yoki tanishib chiqishini nusxalashi mumkin.

3. Insayder ishchi ma'lumotlarga ruxsatnomasi yo'q, ammo unga ega bo'lish uchun o'z ish faoliyatida o'zgarishlarni motivasiya qilib ushbu ma'lumotlarga erishish yo'llarini qidirib chiqishidir.

4. Insayder ruxsatnomasi bo'lmay turib ma'lumotlarni qo'lga kiritishida tizimning zaif jihatlaridan foydalanadi yoki ma'lumotlarni saqlash qurilmasini o'g'irlash dasturlari yordamida olib boradi.

5. Insayder axborot tizimida administrator vazifasini bajaradi, almashadigan ma'lumotlar bo'lsa unga tanishuv yoki nusxalab olish tarzida taqdim etiladi.

6. Insayder ishchi ma'lumotlarni boshqa ushbu ma'lumotlarga ega insayder bilan og'zaki so'zlashuv vaqtida bilib oladi.

7. Insayder ma'lumotlarni tahlil qilib yoki boshqa ma'lumotlarni birlashtirgan tarzda topadi (masalan xodimlar qanday harakat qilish va h.k.)

8. Insayder ma'lumotlarga boshqa insayder orqali erishadi, bunda ikkinchi insayder yuqorida sanab o'tilgan usullardan foydalangan bo'lishi mumkin.

9. Insayder tomonidan oshkor qilingan ma'lumot yuqorida sanab o'tilgan usullardan foydalangan holda qayta ishlanishi mumkin.

Hisobotlarni soxtalashtirish - bu bilib turib ma'lum bir harakatlardan keyin ma'lumotlarni noto'g'ri aks ettirish. Soxtalashtiriladigan hujjatlar korxonaning ichki hujjatlari yoki tashqi aloqalari hujjatlari bo'lishi mumkin.

Maqsadga qarab hujjatlarni soxtalashtirishni quyidagi guruhlarga ajratishimiz mumkin:

- yashirish yoki aksincha sir saqlash kerak bo'lgan ma'lumotlarni oshkor qilish;
- asl ko'rsatkichlarni yuqori qilib qo'yish yoki kamaytirish, shu yo'l bilan qo'shimcha daromadga ega bo'lish;
- tashkilot xodimlarini xato qilishga chorlash;
- o'zaro shartnoma tuzgan tashkilotlarni xato qilishga chorlash.

Aktivlarni o'g'irlash (moliyaviy yoki material) - bu ongli ravishda tashkilotga tegishli bo'lgan mol-mulkni o'ziga yoki boshqa shaxslar foydasiga hal qilish hisoblanadi.

Material jihatdan o'g'irlash quyidagi jazo guruhlarga bo'linadi:

- o'g'irlik;
- aktivlarni o'zlashtirish yoki ishlatib yuborish;
- har xil buzg'unchi yo'llar bilan tashkilotda asosiy yoki qo'shimcha maqsadlarga erishish;

Buzg'unchilikning quyidagi usullari ko'p tarqalgan:

- material yetkazib beruvchilardan foydalanib buzg'unchilik qilish;
- mijozlar muomalasidan foydalanib buzg'unchilik qilish;
- kredit yoki investisiyalar buzg'unchiligi;
- veksel buzg'unchilik;
- bank kafolati yoki kafolat xatidan foydalanib buzg'unchilik qilish;
- hisob raqamlari bilan buzg'unchilik;
- to'lov hujjatlarini soxtalashtirib yoki o'zgartirib buzg'unchilik qilish;
- plastik kartalar bilan buzg'unchilik (soxta kartalar va operasiyalar);
- depozit buzg'unchiligi;

- tashkilot ichki mol-mulk xo'jaligi faoliyatidan kelib chiqqan holda buzg'unchilik qilish, ko'pchilik hollarda ish kelishuvi asosida.

Tashkilot ishiga qarshi borish (Sabotaj) - bu tashkilot faoliyatiga bilib turib qarshi borish, oqibatda tashkilot qandaydir maqsadlarga erishishi imkonsiz bo'ladi.

Tashkilot ishiga qarshi borish quyidagicha guruhlanishi mumkin:

- tashkilot obro'sini tushirish, masalan ma'lum bir xizmatlar sifatini yomonlashtirish yoki boshqacha yo'l bilan zarar yetkazish;
- tashkilot xodimlariga nisbatan noto'g'ri qarorlarni qabul qilish va shu yo'l bilan ish unumdorlini kamaytirish;
- aloqalarni uzish, yomonlashtirish, yoki har xil usullar bilan biznes boshqaruvga to'sqinlik qilish. Masalan, bozor sharoitida raqobatchi tomon o'zida ustunliklar hosil qilish uchun shunday usullardan foydalanishi mumkin;
- xavfsizlik tizimlariga zarar yetkazish, xavfsizlik tizimlarida ojiz qismlarni yaratish, buning natijasida tashkilot aksiyalariga zarar yetishi mumkin;
- izlarni yashirish yoki soxta izlarga olib borish, tergov ishlarini olib borish uchun to'sqinlik qilish;
- qimmatli qog'ozlar bozorida manipulyasiya ishlarini amalga oshirish natijada negativ holatni yaratish;
- tashkilotdan yoki ma'lum bir xodimlardan qasd olish;
- ekstremistik-terroristik, siyosiy yoki shunga o'xshash maqsadlar;
- qoidabuzarlikni yashirish - bu qoidabuzarlikni aniqlashda to'siq hosil qilib uni yashirish yoki yashirishda ko'maklashish hisoblanadi;
- yashirin qoidabuzarlik va shu bilan birga boshqa qoida buzarliklar qastdan amalga oshirilishi mumkin, bunda har xil hujjatlarni soxtalashtirish, ma'lumotlarni o'chirib tashlash yoki yo'q qilish mumkin.

Lavozimdan yovuz maqsadlarda foydalanish - bu insayder tomonidan o'z ish lavozimidan o'ziga nisbatan yaxshi vaziyat yaratishda foydalanish hisoblanadi. O'z lavozimini suiste'mol qilishga quyidagilar kiradi:

- manipulyasiya, xizmat ko'rsatishga bog'liq, masalan ma'lum bir mijozlar uchun bozorda yomon sharoit yaratib o'z obro'sini oshirish;
- sotib olish ishlari bo'yicha manipulyasiya, ma'lum bir mahsulot yetkazib beruvchilar uchun yaxshiroq sharoit yaratish;
- tashkilot faoliyati orqali manipulyasiyasi.

O‘z lavozimini suiste’mol qilish orqali xar bir hodim o‘zi bilib bilmay tashkilot uchun juda katta zarar keltirish mumkin. Shuning uchun ham hodimlarga ichonch bildirishdan oldin albatta tekshirib ko‘rish maqsadga muvofiq bo‘ladi.

3.4. Axborot xavfsizligi insidentlarini nazorat etuvchi vositalarning tahlili

Bugungi kunda milliy axborot tizimlarimiz va internetdan foydalanuvchilar uchun yagona markaz bo‘lgan ushbu xizmat tomonidan axborot to‘plash, tahlil qilish, maslahat berish hamda texnik ko‘maklashish borasida salmoqli ishlar amalga oshirilmoqda.

Milliy axborot tizimlari va internetdan foydalanuvchilar uchun yagona markaz bo‘lgan UZ-CERT tomonidan axborot to‘plash, tahlil qilish, maslahat berish hamda texnik ko‘maklashish borasida salmoqli ishlar amalga oshirilmoqda.

UZ-CERT xizmati mutaxassislarining aytishicha, barcha tashkilot faoliyatini batafsil o‘rganish, muvofiqlashtirish kiber-tahdidlarga qarshi kurashga yordam bermoqda. Internet-firibgarlik yoki foydalanuvchilar maxfiy ma’lumotlaridan noqonuniy foydalanish eng keng tarqalgan ana shunday xavflardan hisoblanadi. Bunday qing‘ir maqsadlarga, odatda, servis ichida mashhur brendlar nomidan elektron xatlar va shaxsiy ma’lumotlarni ommaviy tarqatish orqali erishiladi.

Kiber-jinoyat butun dunyoda oddiy jinoyatlarga tenglashtirilmoqda, ularni sodir etgan shaxslar esa qonun bo‘yicha jazolanmoqda. Jinoyatga daxldorligi ekspertiza tomonidan aniqlanadigan kompyuter, axborot manbalari – disklar, fleshkalar, IP-manzillar, tarmoq uskunalari tegishli ayblarni qo‘yishda dalil bo‘lishi mumkin. UZ-CERT xizmati xodimlari kiber-jinoyatni tekshirishda jinoyat izini yashirish maqsadida yo‘q qilingan ma’lumotlarni qayta tiklaydi.

UZ-CERT xizmati holatlarini tahlili

Mavjud resurlardan samarali foydalanish uchun va axborot tizimlari, Datamarkazda joylashgan mijoz veb-saytlarini va UZINFOCOM Markazi xizmatlari iste’molchilarini ximoyalanganlik darajasini oshirish maksadida, hamda zararli kompyuter insidentlariga tezkor javob ko‘rish va ularning oqibatlari va sabablarini bartaraf qilish

maqsadida UZINFOCOM Markazida UZ-CERT (UZINFOCOM Markazining kompyuter insidentlariga tezkor javob qaytarish xizmati) nomi ostida texnik xavfsizlik bo'limi xizmat ko'rsatmoqda.

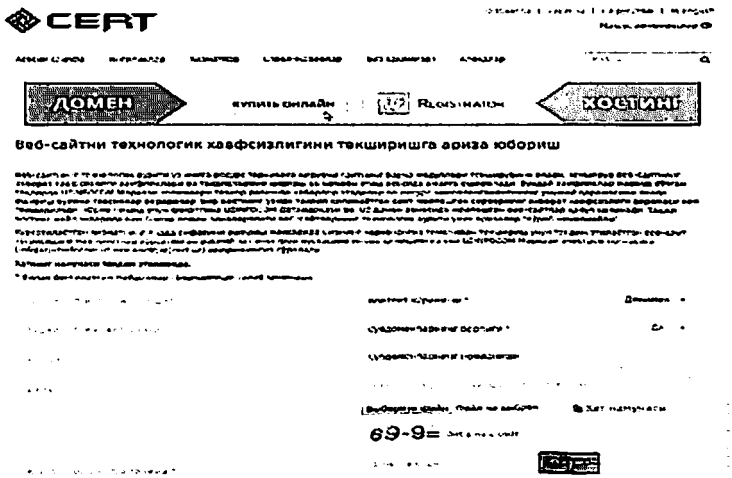
UZ-CERT xizmati Datamarkaz mijozlariga yuqori darajali xizmatlar ko'rsatishga yo'naltirilgan. Bundan tashqari so'rov asosida korxonalar va tashkilotlarning axborot tizimlarini xavfsizligini ta'minlash va ro'y beruvchi kompyuter xodisalarini bartaraf etish va oldini olishda ko'maklashib kelmoqda. Shuni ta'kidlash lozimki UZ-CERT xizmati davlat nazorat organi emas va tekshirishlar natijalari tavsiya xarakteriga ega.

Bugungi kunda mavjud ko'rsatiladigan xizmatlar ro'yxatiga quyidagilar kiradi:

- Axborot xavfsizligi ekspertizasini o'tkazish;
- Axborot xavfsizligi siyosatini ishlab chiqish;
- Veb-saytni texnologik xavfsizligini tekshirish;
- Fayllarni virusdan tekshirish;
- Serverlardagi axborot xavfsizligi holati analizi xamda boshqalar.

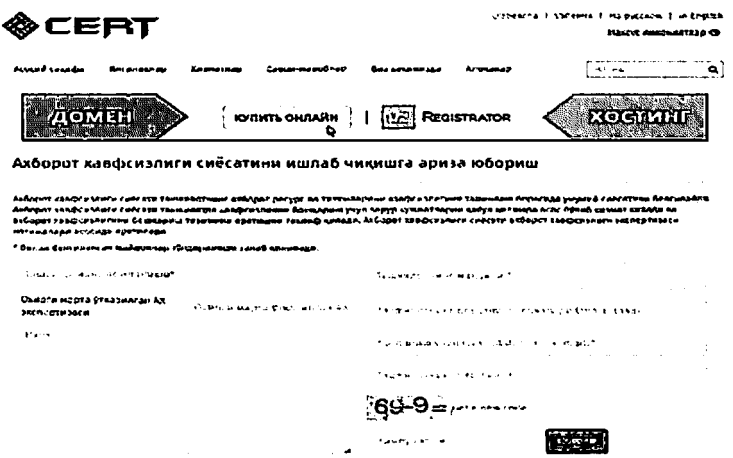
Tashkilot o'z faoliyati doirasida konfidensial ma'lumotlar bilan ishlasa (xodimlar yoki mijozlar ma'lumotlari) AX ekspertizasini o'tkazish o'ta muximdir. Bu turdagi ma'lumotlarni tashqi kirishlardan himoyalash shunchaki extiyotkorlik emas, balki tashkilotning asosiy majburiyatlaridan biridir.

UZ-CERT mutaxassislari tomonidan o'tkaziladigan AX ekspertizasi ma'lumotlar muhimligi darajasi, konfidensial axborotlarni saqlash obyektlarining tahlili va ularni saqlash obyektlariga kirish yo'llarini aniqlashni, korporativ muhitda yechilayotgan masalalarni tekshirishni, operasion tizim, tarmoq xizmatlari protokollari va himoya tizimlari analizini o'z ichiga oladi.



3.2-rasm. UZ-CERT tashkiloti ko'rsayatayotgan xizmatlari

O'tkazilgan, tarmoq va tizim axborot xavfsizligini ekspertizasi asosida, UZ-CERT mutaxassislari, tashkilotning axborot resurslari himoyasini kerakli darajaga oshirish imkoniyatini beruvchi tavsiyalar beradilar.



3.3-rasm. UZ-CERT tashkiloti ko'rsayatayotgan xizmati (AX siyosatini ishlab chiqish)

Axborot xavfsizligi (AX) ekspertizasi tashkilotlarning kompyuter tizimlarini kamchilik va zaifliklarini aniqlash maqsadida amalga

oshiriladi hamda ularning ish samaradorligini baholash va tashkilotning axborot himoyasini tahlilini tashkil etish maqsadida quyidagi ishlarni amalga oshiradi:

- tizimning mavjud meyoriy talablarga mosligini baholash;
- xavfsizlik sohasida qabul qilinayotgan barcha yechimlarni asosli va xuquqiyligini aniqlash.

3.4-rasm. UZ-CERT tashkiloti ko‘rsayatayotgan xizmati

AX ekspertizasi quyidagi bosqichlardan iborat:

- ishchi stansiyalarni tashqi nazorati;
- serverlarni tashqi nazorati;
- ishchi stansiyalar va serverlarni lokal tarmoq doirasida zaifliklar mavjudligiga maxsus dasturiy ta’minot bilan skanerlash;

- mavjud veb-saytlarni zaifliklar mavjudligiga avtomatlashtirilgan dasturiy ta'minot bilan skanerlash va standart qo'losti vositalari yordamida tekshirish;

- o'rganilayotgan axborot tizimi joylashgan hududda mavjud jismoniy himoyaning tahlili;

- mavjud ichki meyyoriy xujjatlarnining taxlili, xususan axborot himoyasi doirasida;

- tashkilotdagi javobgar shaxslarni so'rovdan o'tkazish;

- ommaviy resurslarni va tarmoqda aylanayotgan ma'lumotlarning tahlili.

Amerika va Yevropa mamlakatlarida axborot xavfsizligi insidentlarini tergov qilish yetarlicha rivojlangan bo'lib bu borada katta ishlar va xizmatlar yo'lga qo'yilgan.

Amerika Qo'shma Shtatlarida AX insidentlarini tergov qilish va shaxsiy ma'lumotlarni himoyalash servisining bozordagi qiymati bir necha milliard dollar qiymatni tashkil etadi.

Sohaning predmet qismi quyidagilardan iborat:

- Insidentlarni tergov qilish (kompyuter jinoyatlari): ichki va tashqi insident, insident qanday sodir bo'lgan, nima sababli sodir bo'lgan, aybdorlar kimligini aniqlash;

- Insidentga reaksiya va uning monitoringi: insident sodir bo'lish vaqtida zararni minimallashtirish, dalillarni to'g'ri yig'ish va insidentni qanday aniqlash;

- Kompyuter kriminalistikasi: loboratoriya kompyuter kriminalistikasi – hodisalar ketma-ketligini tiklash, ma'lumot tashuvchilarda dalillarni qidirish, ma'lumotlarni qayta tiklash;

- Barcha ishlarni yuridik olib borish: barcha ishlar qonun doirasida olib borish

RU-CERT – kompyuter insidenlariga javob qaytarish markazi bo'lib, uning asosiy vazifasi – Internetning Rossiya segmetida foydalanuvchilar uchun AX tahdidlar sodir bo'lish darajasini kamaytirishdan iborat.

RU-CERT resurslarni yopish, manzillarni filtrlash, domenlarni yopish, u yoki bu resurs kontentini o'chirish, u yoki bu hodisalarga aloqador shaxslarni izlash vakolatlariga yega emas.

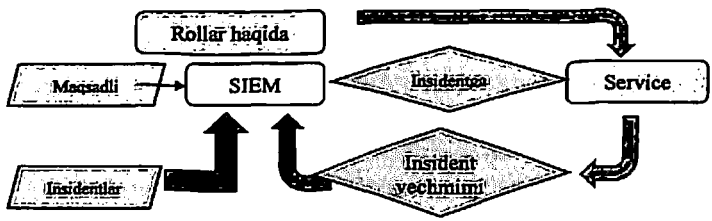
RU-CERT insidentga javob qaytarish servisini hech qanday kafolatsiz amalga oshiradi.

US-CERT boshqarish prinsipi natijasida quyidagi vazifalar bajarilishi va samaralarga erishishi mumkin:

- Axborotning yuqori sifatligi;
- Yaxshilangan axborot xabardorligi;
- Insidentga tezkor javob qaytarish.

AX insidentlarini nazorat etish tizimlari – bu insidentlarni lokalizasiyalash va zarani kamaytirishni ta'minlovchm vositalar hisoblanadi. Bu vositalar kompyuter insidentlari natijasidagi zaralarni kamaytirish bo'yicha oldindan ishlab chiqilgan avtomatlashtirilgan ssenariylarga ega yoki masofadan o'z konfigurasiyalarini o'zgartirish imkoniyati mavjud bo'lgan mexanizmga ega bo'ladi.

SIEM (Security information and event management) – AXni boshqarish va xavfsizlik hodisalarini nazorat etish.



3.5-rasm. SIEM asosidagi insidentlarni nazoratlash jarayonini avtomatlashtirish tizimi

AX insidentlari reaksiya va monitoring Markazi (SOC) dan foydalanganda quyidagi samaralarga erishishi mumkin:

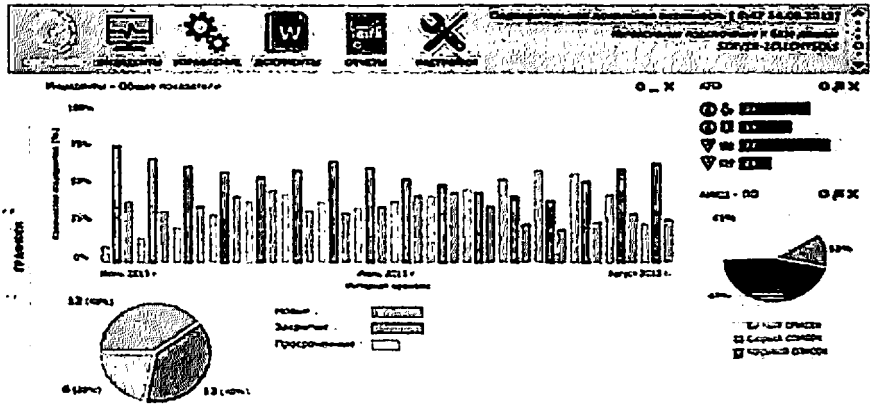
- AX ta'minlashni tayyor jarayoni;
- Kapital xarajatlarni yo'qligi;
- Investisiya yuqoriligi;
- Sifatni oshishi;
- Inson resurslardan ozod bo'lish.

AX insidentlari reaksiya va monitoring markazi keng doirali AX servislarini taqdim etadi:

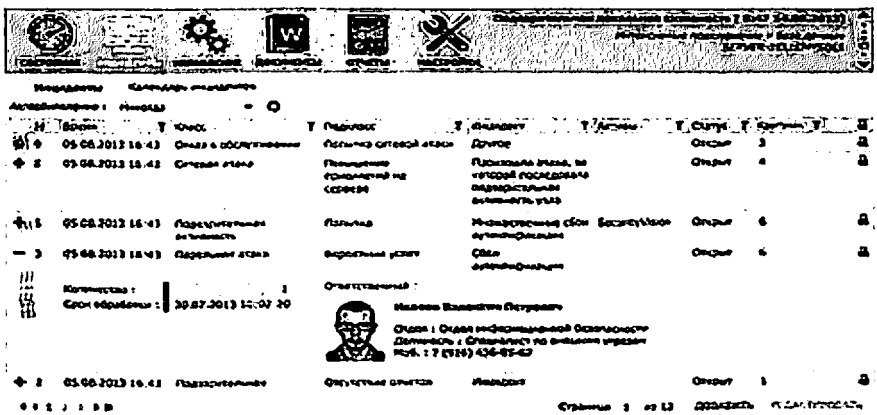
AX insidentlarini nazorat etuvchi vositalar – bu tizimning boshqa jarayonlari bilan chuqur integrallashgan tizimdir.

Insidentlarni nazorat etish vositalari amalga oshirish uchun ko'plab yuzaga keladigan muammolarni yechish lozim.

Bunday tizimlar ko'plab funsiyalarni o'z ichiga olishini hisobga olgan holda interfeysda namoyish etiladigan ma'lumotlar to'plami ham keng qamrovli bo'lishi lozim.



3.6-rasm. Insidentlarni nazorat etuvchi tizimi interfeyiga misol



3.7-rasm. Insidentlarni kuzatish va javobgar xodim to‘g‘risida ma’lumotni ko‘rsatish

Insidentlarni nazorat etish tashkilotning kopleks xavfsizligini ajralmas qismi hisoblanadi.

AXni boshqarish siyosati tarkibiga jarayonning kuzatish, unga jalb etilgan bo‘limlar, javobgarlar, reaksiya vaqti, hisobot formalari kabi ma’lumotlar kiradi.

3.5. Jarayonlar o'rtasida rollarni taqsimlash va insidentni boshqarish jarayonidagi xodimlarni aniqlash

Boshqaruv guruhi tomonidan qo'llab-quvvatlashga erishilgandan so'ng menejment insidentlarini boshqarish zarurligi va insidentni boshqarish uchun vazifalarni qanday taqsimlanishi masalasini ko'rib chiqishga to'g'ri keladi. Quyidagi 1-jadvalda ko'p uchraydigan lavozimlar va u yerda rol va qanday vazifalar bajarilishi keltirilgan.

1-jadval.

Vazifa va majburiyatlar

	Lavozim	Vazifa	Majburiyat
1.	Axborot xavfsizligi ta'minlash bo'yicha vakolatli tashkilot	Bu tuzilma axborot xavfsizligi sohasida to'laqonli huquqlarga ega	1. Insidentni boshqarish bo'yicha javobgar. 2. Insidentni boshqarish bo'yicha reja ishlab chiqish. 3. Istisno va moslashtirish. 4. Oxirgi qarorni qabul qilish.
2.	Axborot xavfsizligi bo'yicha menejment	Insidentni boshqarish guruhi rahbari va AX markazi bilan bog'lab turuvchi shaxs	1. Insidentni boshqarish bo'yicha rejalarni ishlab chiqish va amaliyotga tadbiq etish. 2. Xavflarni va insidentlarni to'g'ri boshqarish. 3. Axborot xavfini boshqarishda proaktiv va aktiv harakatlarni amalga oshirish.
3.	Insidentlarda javob qaytarish menedjeri (bazi	Insidentlarga javob qaytarish bo'limi boshqaruvchisi	1. Insidentlarga javob qaytarish bo'limi

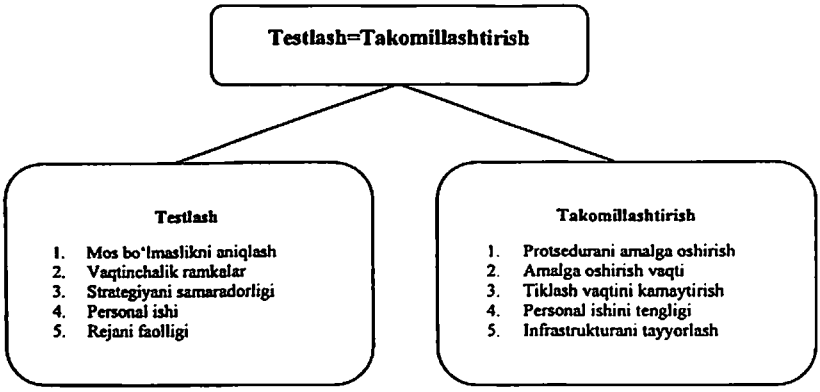
	hollarda AX menedjeri hisoblanadi)		boshqaruvchiligi. 2. Xodimlar harakatlarini kordinasiya qilish. 3. Insidentlarga javob qaytarish rejalarni muvaffaqiyatli tugashi javobgari. 4. AX markaziga insidentlar haqida xisobot topshirish.
4.	Axborot xavfsizligi insidentlariga javob qaytarish guruhi azosi	Guruh ishlarida qatnashish	1. Insidentlar zararini minimallashtirish. 2. Insidentlarga javob qaytarishda ketma-ket harakatlarni hujjatlashtirib borish. 3. Insident yuz berganda sudlashuv holati uchun dalillar zanjirini saqlab borish. 4. Insidentga qanday javob qaytarilgani haqida hisobot yozib borish.
5.	Tergovchi	Kutilmagan insidentlar guruhi azosi	1. Kutilmagan insident tergovini olib boradi. 2. Insident sababini aniqlaydi. 3. Tergov haqida xisobot tayyorlaydi.

6.	AX bo'yicha AT mutaxasis	Axborot xavfsizligi insidentlariga javob beruvchi guruh a'zosi.	1. Insidentda tergovni amalga oshirish. 2. Xavfsizlikni ta'minlash uchun qo'shimcha chora-tadbirlarni amalga oshirish.
7.	Biznes bo'lim boshqaruvchisi	Biznes jarayon va aktivlar egasi	1. Jarayon/resurs/tizim haqida insidentlar guruhi maslahatlaridan kelib chiqqan holda qarorlar qabul qilish. 2. Aktivlarni tiklashni aniqlash va biznes jarayonlarda tahdidlarni baholashini o'tkazish.
8.	AT mutaxassis	AT bo'limi xodimi	1. Insidentlarni yo'qotish jarayonida axborot xavfsizligi insidentlariga javob beruvchi guruh a'zosiga yordam berish. 2. Tasdiqlangan qoida va siyosat asosida korxona axborot tizimini qo'lab-quvvatlash.
9.	Huquqshunos	Huquqlar bo'limi xodimi	Boshqarish/javob qaytarish/tergov vaqtida yordam beradi.

10.	Kadrlar bo'limi hodimi	Xodimlarni boshqarish bo'limi mutaxassisi	1. Boshqarish/javob qaytarish/tergov vaqtida hodimdan shubha qilinsa yordam beradi. 2. Insidentni boshqarishga tegishli aspektlarni boshqarish siyosatini qurish.
11.	Press-kotib (a)	Ommaviy axborot vositalari bilan ishlash mutaxassisi	Brendlarni saqlashni va korxona obro'sini, OAV ni, va aksionerlar insidentini saqlash maqsadida axborot taqdim etish.
12.	Xavflarni tahlil etuvchi mutaxassis	AX bo'limi xodimi, xavflar bo'yicha ichki boshqaruv yoki xavflarni boshqarish	1. Xavflarni kamaytirish va ularni boshqarish uchun bo'lim boshliqlari bilan birga ishlash. 2. Asosiy ma'lumotlarni taqdim etish (xavflarni boshqarish strategiyasi).

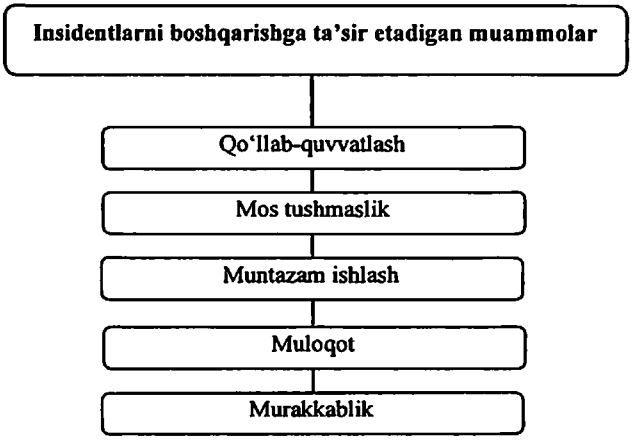
Asosiy kalit vazifalarini aniqlab olganimizdan so'ng, insidentlarni boshqarish jarayonini hujjatlashtirish kerak bo'ladi.

Istalgan jarayondagi kabi insidentlarni boshqarish ham jarayoni siklik ravishda doimo rivojlanib borishi zarur (3.8-rasm).



3.8-rasm. Testlash va yaxshilash

Istalgan jarayonni boshqarishda shu jarayonning qiyin nuqtalari mavjud bo'ladi. Ushbu muammolarni hal qilish esa ishning qanchalik unumdor bo'lishini aniqlab beradi. Tajribadan kelib chiqqan holda quyidagi muammolarni ajratib oldik (3.9-rasm).



3.9-rasm. Axborot xavfsizligi insidentlarini boshqarishda yuzaga keladigan muammolar.

Insidentlarni boshqarish qiyin jarayon hisoblanib, hodimlardan birga va aniq ishlashni talab qiladi. Har qanday insident juda katta muammoga aylanib ketmasligi uchun oldindan belgilangan qoidalarga to'laqonli amal qilish zarur bo'ladi.

Jarayon to'g'ri borishi 90% hodimlarga bog'liq bo'lgani uchun asosiy e'tiborni kutilamgan insidentlarga qanday javob qaytarish va ish faoliyatini qanday tiklash rejalarini tashkil qilish masalasiga qaratish lozim.

Insident quyidagi qoidalarga amal qilishi lozim:

- xodimlar va mehmonlar xavfsizligi;
- insidentni minimal zarar bilan ushlab turish;
- tashkilot aktivlari xavfsizligi;
- axborot texnologiyalari xavfsizligi;
- biznes talablaridan kelib chiqib ishni tiklash;
- insident tergovi;
- shunday insident qayta takrorlanmasligi uchun chora-tadbirlar.

Ushbu qoidalar axborot xavfsizligi insidentlari jarayonini samarali boshqarishni qurishga amaliy yordam beradi.

3.6. Axborot xavfsizligi insidentlarini presedentli tahlili

Umumiy xolda insidentlarni boshqarish siklik jarayon bo'lib uning asosiy bosqichlarini PDCA modeli aks ettiradi. ISO 27001 standartiga asosan an'anaviy model boshqarishni to'rtta bosqichidan iborat:

- axborot xavfsizligi insidentlarini identifikatlashtirish;
- axborot xavfsizligi insidentlariga aks ta'sir ko'rsatish;
- tergovni amalga oshirish;
- korreksiyalovchi va oldini olish tadbirlari

Insidentga aks ta'sir ko'rsatish va tergovni amalga oshirish paytida axborot tizimini konkret zaifliklari aniqlashtiriladi, ruxsatsiz kirish va hujum izlari namoyon bo'ladi, ximoya vositalarining imkoniyati tekshiriladi, tizim arxitekturasini (buzilishi) axborot xavfsizligi sifati va uni boshqarish mumkinligi aniqlanadi. Shuningdek taxlil qilish proseduralarining mavjudligi va insident oqibatlarini oldini olish va qaytarilish extimolligi kamaytirish choralari ko'rilishidir. Birinchi navbatda sodir bo'lishi mumkin bo'lgan insidentni o'z vaqtida aniqlash lozim. Aks xolda qisqa muddatda aks ta'sir ko'rsatish mumkin bo'lmay qoladi. Shuningdek aniqlangan insidentlarga nisbatan aks ta'sir ko'rsatish choralari ishlab chiqilmagan. Bunday vaziyatlarni hal qilish uchun ko'p vaqt talab etiladi.

Axborot xavfsizligi insidentlariga aks ta'sir ko'rsatish muammolari. Insidentlarni boshqarishning asosiy vositalariga monitoring tizimi va xodisalarining axborot xavfsizligi korrelyasiyasi

xisoblanadi, tahlil natijalari asosida aks ta'sir strategiyasi ishlab chiqiladi. Monitoring tizimi shakllantiradigan axborotdan katta xajmi, yuqori malakali Mutaxassislardan iborat axborot xavfsizligi insidentlariga aks ta'sir etuvchi guruhning mavjudligini talab yetadi. Moliyaviy imkoniyatlarning yo'qligi va mutaxassislarsiz insidentlarni boshqarish jarayoni samaradorli tashkil yetilishini xar doim xam imkoniyati bo'lmaydi. Qaror qabul qilish ,bosqichida ekspertga fikriga tayanib qolish operativlikni kamaytiradi va natijada talofatni ko'paytiradi. Shunday qilib, yuzaga kelishi mumkin bo'lgan insidentlarga operativ aks ta'sir ko'rsatishdek dolzarb muammo mavjud. Bir qator aniqlangan strategiyalardan birini qo'llash masalasini yechish, yoki mos keladigan strategiya yo'qligini e'tirof etib uni ishlab chiqish. Xaqiqatga yaqinlik uslubi insidentlarga aks ta'sir etish muammosi yechimini topishda boshqarish jarayonini avtomatlashtirish vositalari sifatida presedent (CBR) asosidagi tizimlarni taqazo etadi. Natijada insidentlarga aks ta'sir etishni aniqlash faoliyatini avtomatlashtiradi, samaradorligini oshiradi, aks ta'sirni amalga oshirishini tezlashtiradi va axborot xavfsizligini boshqarish jarayoniga intellektual yondashish imkonini beradi.

Presedentli taxlil. Presedentli tizimlarda yechimni qidirish analog tushunchasiga tayanadi (xususiydan xususiygacha qidirish). Presedent va joriy vaziyat obyekt sifatida tasvirlanadi, ular uchun analogni topish zarur va presedentlar uchun zarur va presedentlar uchun adolatli faktlarni ko'chirish evaziga, ko'rinayotgan insident uchun qisman xulosa qilish.

Odatda presedent tashkil topadi:

- muammoli vaziyatning izoxidan;
- muammoni bartaraf etish uchun ko'rilayotgan harakatlardan to'planadi;
- va bazi xollarda- natija (yoki prognoz) ni yechimini qo'llash.

Presedentning muqobil tuzilmasini ko'p o'lchamli parametrik vektor ko'rinishida ko'rsatish mumkin.

$$CASE = (x_1, x_2, \dots x_p, R),$$

Bunda $x_1, x_2, \dots x_p$ – vaziyat parametrlari, ushbu presedentni izoxi.

R –masalaning bir yoki bir necha yechimlar to'plami (diagnoz, tavsiyalar). Presedentlar asosida muloxaza to'rtta asosiy bosqichni tashkil etuvchi CBR –sikl (presedentlar asosida muloxaza sikli), bo'lib quyidagilardan iborat:

- yuzaga kelgan vaziyat uchun presedentlar bazasidan mos presedentlarni ajratish;
- joriy muammoni yechimini topish uchun presedentdan qaytadan foydalanish;
- yechimni qayta ko'rish va joriy muammoga mos ravishda moslashtirish;
- qabul qilingan yechimni yangi presedent qismi sifatida saqlash.

Konkret predmet soxa spesifikasiyasini va yechiladigan masalani xisobga olgan xolda soddalashtirilgan CBR –sikl qo'llanishi mumkin.

Shunday qilib, presedentlar apparatini qo'llashdan maqsad operatorga tayyor yechimni chiqarib berishdan iborat. Presedentlarni ajratish moslik funksiyasini aniqlashga asoslangan, uning qiymati joriy vaziyatni va presedentni o'xshashligini aniqlaydi. Belgilar fazosida maqsadni funksiyaga mos nuqta aniqlanadi va o'lchov doirasida eng yaqin presedent olinadi.

Formal nuqtai nazardan presedent o'xshashligi $g = (x_{g1}, x_{g2}, \dots x_{gp})$ va joriy vaziyat $k = (x_{k1}, x_{k2}, \dots x_{kp})$ qùyidagi funksiya ko'rinishida ifodalanadi.

$$SIM(g,k) = F\left(sim(x_{g1}, x_{k1}), \dots, sim(x_{gp}, x_{kp})\right)$$

Bunda $sim(x_{gi}, x_{ki})$ presedentdan i- belgisini qiymatini va k joriy xodisadan (insident) i-belgisi lokal o'xshashligi. F funksiya presedentdan joriy vaziyat bilan to'liq mosligini ifodalaydi. Bazada o'xshash presedentlar yo'q bo'lganda, ushbu usul yuzaga kelgan vaziyat uchun yechimni topmaydi. Ushbu muammoni hal qilish uchun CBR – siklda bazani xulosa qilish jarayonida to'ldirish imkoniyati nazarda tutilganda yechimi topiladi.

Presedentli taxlilni qo'llash konsepsiyasi.

Yuqorida aytib o'tilganidek axborot xavfsizligi insidentlarini boshqarishning birinchi qadami insidentlarni ro'yxatga olishdir. Keyingi harakatlar har bitta insident uchun klassni xisobga olgan xolda aks ta'sirni qo'llashni tahlil qiladi. Ushbu bosqichda quyidagi muammolarni ajratish mumkin.

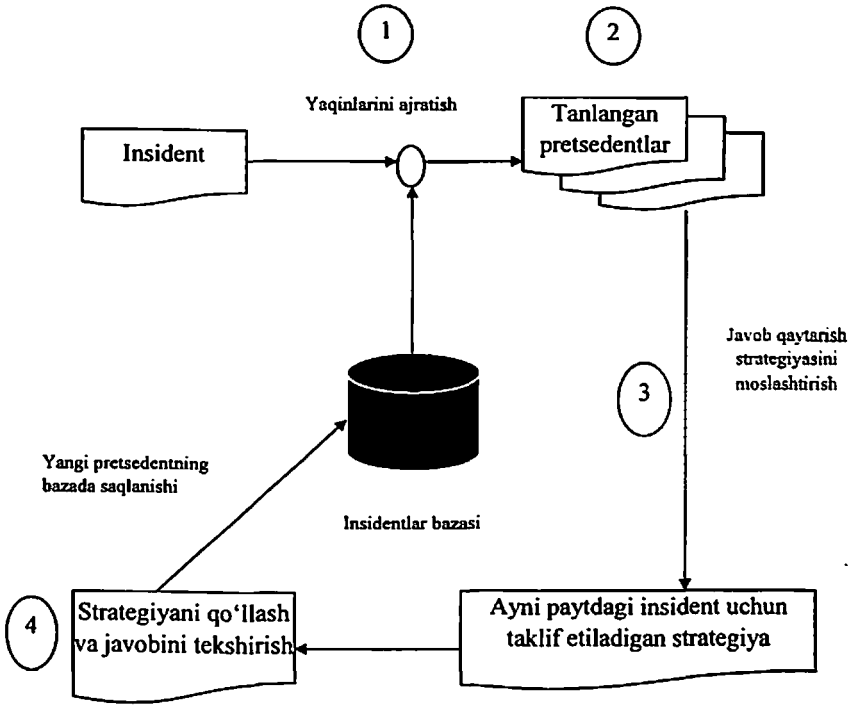
1. Har doim ham insidentlarni klassifikasiyalash to'g'ri bajarilmaydi.
2. Har bitta insident o'zgacha belgtlarga yega bo'lganligi uchun ma'lum toifali insidentlarga aks ta'sirdan yagona strategiya mavjud emas.

3. Oldin sodir bo'lmagan insidentlar yuzaga kelishi mumkin shuning uchun bunday insidentlar uchun mos ravishda aks ta'sir strategiyasi mavjud emas.

Insidentlarni boshqarish jarayonini takomillashtirish uchun insidentni tahlil konsepsiyasini qo'llash quyidagilardan iborat. Ma'lum bo'lgan G - insidentlar to'plami aniqlangan R aks ta'sir strategiyalari to'plami mavjud. $G \rightarrow R$ ga akslanishi presedent ya'ni insidentning izohi va unga mos ravishda ta'sir strategiyasi turidagi juftlik. YA'ni insidentni ro'yxatga olganda unga mos ravishda presedent topiladi. Shundan so'ng presedent yechimi ushbu insident uchun qo'llanadi. Ushbu uslubni amalga oshiruvchi tizimning mantiqiy tuzilishi 3.11-rasmda keltirilgan.

Oldin ma'lum bo'lmagan insidentlar va ular uchun aks ta'sir strategiyasi yo'q bo'lgan insidentlarni anomal insidentlar deb ataymiz. Boshqacha qilib aytganda anomal insident deganda himoya vositasi belgilangan insidentga klass doirasida o'xshashi bo'lmagan insidentga aytiladi.

Insidentni anomalligi to'g'risidagi xulosa har tomonlama tahlil qilish uchun asos bo'ladi. Shularni hisobga olgan holda presedentli tahlil insidentlarni normal va normal bo'lmagan sinflarga ajratishni nazarda tutadi.



3.10-rasm. Presedentli tahlil tizimining mantiqiy tuzilishi.

$G = \{g_1, \dots, g_n\}$ – presedentlar to'plami;

$g_i = (x_1, \dots, x_p, r_i)$ – yagona presedent;

$K = \{k_1, \dots, k_m\}$ – ro'yxatga olingan insidentlar to'plami;

$k_j = \{x_1, \dots, x_p\}$ – bitta insident;

$F(g_i, k_j)$ – o'xshashlik funksiyasi;

$G_1 = \{g_i : F(g_i, k_j) \le d_{lim}\}$ – o'xshash presedentlar to'plami.

Shunday qilib insidentni presedentlar to'plamiga o'tkazish sharti quyidagicha ifodalanadi:

$$k_j \in G \leftrightarrow |G_1| \ge a_{lim}.$$

Ifodadan ko'rinib turibdiki sinflarga bo'lish natijasi chegaraviy masofadan d_{lim} va o'xshashliklarning a_{lim} ning eng ko'p qiymatiga to'g'ridan to'g'ri bog'liq.

Presedentli tahlil algoritmining modeli. Tavsiya etilgan usulning samaradorligini tadqiq etish uchun KddDataset'99 ma'lumotlar manbaidan foydalaniladi. Metrik sinflash sifatida k –yaqin qo'shnilar metodi qo'llanildi. Ushbu bosqichda oxirgi natijaga har bir

parametrning ta'siri ma'lum bo'lmaganligi uchun, o'lchov birlikni og'irlik koeffisentlarisiz olish maqsadga muvofiq. Matnli ssenariyning algoritmi DeductorStudioAcademic tahlil platformasidan tashkil topgan (3.12-rasm).

Ro'yxatga olingandan so'ng normalisasiya o'tkaziladi.

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}}.$$

1. Algoritm parametrlarini inisializasiyasi: metrikani tanlash, d_{lim} masofa chegarasini va a_{lim}ga analog chegara qiymatini aniqlash.

d_{lim} ni boshlang'ich qiymati sifatida sinf masofasi kiritilgan:

Bu yerda, bitta presedentdan sinfgacha o'rtacha masofa

$$d_{cp} = \frac{\sum_{i=1}^{n} d_{i_{cp}}}{n},$$

2. Metrika bo'yicha obyektlar orasidagi oraliqni hisoblash

$$d_{i_{cp}} = \sqrt{\sum_{i=1}^{p} (x_{gi} - x_{ki})^2}.$$

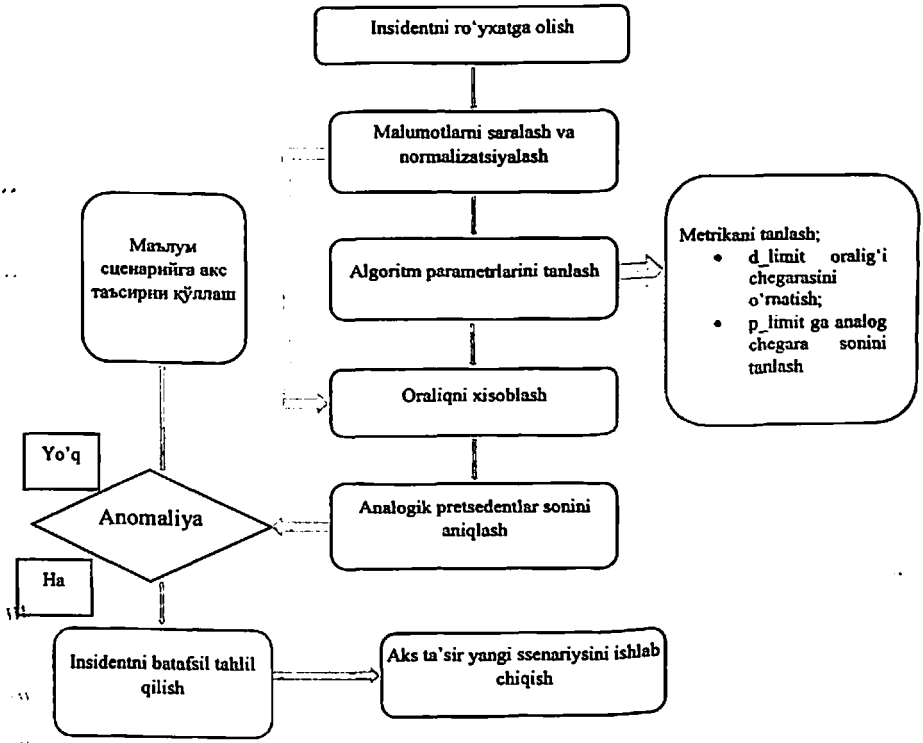
3. $d_{gk} \leq d_{lim}$ ifodani qanoatlantiruvchi ikki obyektni aniqlash. (presedent g va k insident o'xshash hisoblanadi.

4. $d_{gk} \leq d_{lim}$. shartni bajaruvchi har bir k_j Insidentga a presedentlar soni hisoblanadi.

5. Insident k_j $a \leq a_{lim}$. bo'lganda anomal deb ko'riladi.

6. Tasniflash natijasidan kelib chiqib keyingi choralar ko'riladi.

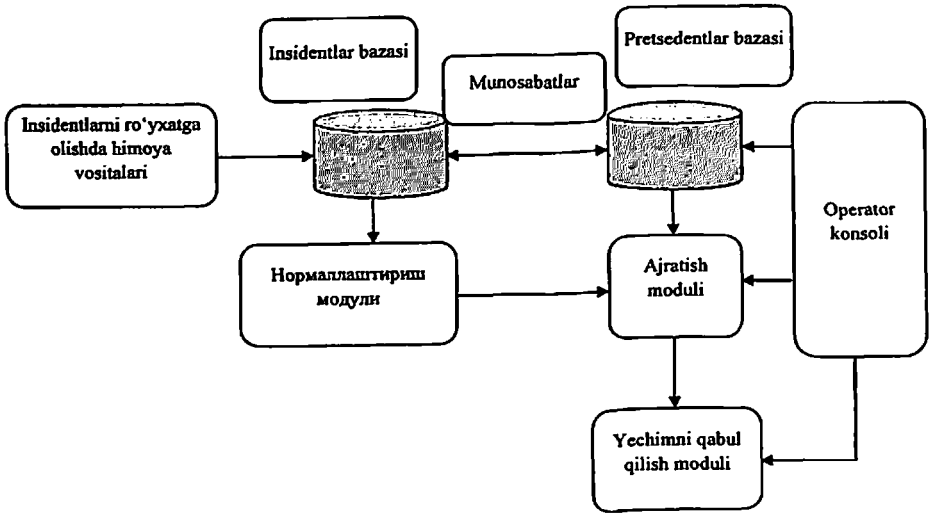
7. Insidentlarni batafsil tahlili yoki aks ta'sir strategiyasini qo'llash.



3.11-rasm. Matnli ssenariyning algoritmi.

Presedentli taxlil tizimi arxitekturasi. Presedentli tahlil tizimini dasturiy ishlab chiqilishiga ko'ra, modulli tuzilishga yega bo'lib quyidagi komponentlardan tashkil topgan.(3.13-rasm):

- ro'yxatga olingan qayta ishlash uchun tayyorlangan insedentlar bo'yicha yozuvlar, insidentlar bazasi;
- ma'lumotlarni normallashtirish moduli, ro'yhatga olingan insidentlarni, presedentlarni bazasi tuzilishiga ko'ra o'zgartiruvchi;
- ajratish moduli, insident va presedentlarni o'xshashlik kattaliklarini hisoblash funksiyasi;
- qaror qabul qilish moduli, sinflash natijasini aniqlovchi va insidentni bitta yoki bir nechta presedentga kattaliklar mosligi bo'yicha o'xshashlikni o'rnatish;
- operator konsoli, avval no'malum bo'lgan shartlar uchun ishlab chiqilgan strategiyani moslashtirish va tahlil jarayonini korresiyalash uchun mo'ljallangan.

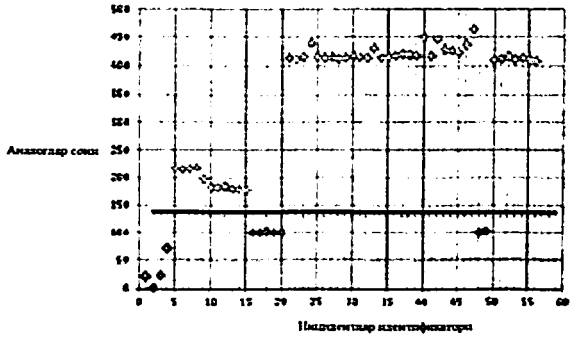


3.12-rasm. Presedentli tahlil tizimi arxitekturasi

Shunday qilib, presedentli analiz konsepsiyasini vosita sifatida qo'llash, axborot xavfsizligi insidentlarini boshqarish jarayonini takomillashtish, insidentlarga nisbatan aks ta'sir operativligini orttirilgan tajribani qo'llash orqali bir necha marta oshiradi. Undan tashqari, bunday yondoshuv har tomonlama o'rganilishi dolzarb bo'lgan anomal insidentlarni aniqlash masalasini hal qiladi.

Raqamli eksperimentlar natijalari. Algoritmni bunday yechilishi natijani analitik ko'rinishda, ham grafik nuqtali diagramma ko'rinishida olish imkonini beradi. Nuqtali diagramma yordamida e'tibor qaratilishi lozim bo'lgan insidentlarni - ya'ni anomal insidentlarni ko'rish mumkin. (3.14-rasm).

Ko'rinib turibdiki, normal insidentlar sifatida sinflarga ajratilgan insidentlar, son jixatidan ko'pgina normal insidentlardan farq qiladi, ya'ni o'xshashliklar sonini yuqori qiymatiga yaqinlashgan. Bu holat ularni har tomonlama tahlil qilishni va yashirin sabablarni aniqlashni, insidentlar natijasining umumiy qonuniyatga buysunmasligi ko'rinadi.

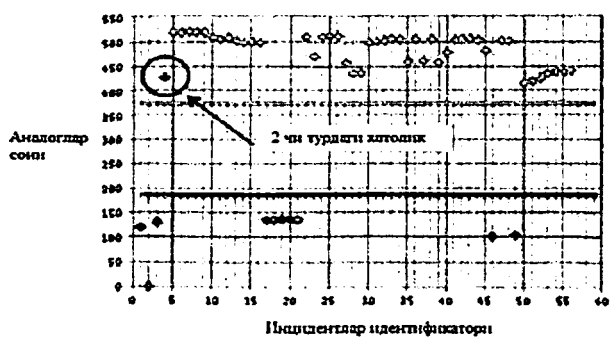


3.13-rasm. Insidentlarni sinflash natijalari

Nul gipoteza insidentning normalligini tahmin qiladi, unda 1-turdagi xato nul gipotezani noto'g'riligini inkor qiladi, 2-turdagi xato nul gipotezani noto'g'ri qabul qilinishidir. d_{lim} va a_{lim} parametrlarni tanlash bir-biriga teskaridir. Bir tomondan, aniqlangan o'xshashliklarning sonini oshishi sinflash aniqligini oshiradi(1-turdagi xatolarni kamaytiradi), lekin bunda sinflar orasidagi chegara unchalik aniq bo'lmaydi. Orasidagi masofani kamayishi aniqroq sinflashtirish imkonini beradi, lekin 2-turdagi xatoliklarni ehtimolligini oshiradi. (3.15-rasm).

Ko'rib turganimizdek bir normal Insident noto'g'ri tasnif qilindi. a_{lim} parametri muayyan vaziyatga bog'liq. Taklif qilingan Insidentlar klassifikasiyasi

Presedentli tahlilning avzalligi yig'ilgan tajribani qayta qo'llash imkoniyati mavjudligi va o'xshash insidentlar uchun aks ta'sir ssenariysi qidiruv vaqtini qisqarishidadir.



3.14-rasm. Insidentlar klassifikasiyasi natijalari

Taklif etilgan konsepsiya muammoli vaziyatlarda batafsil o'rganishni talab yetuvchi o'xshash insidentlarni aniqlashdek masalani yechish va presedentlar bazasida mavjud bo'lgan bilimlar asosida insidentlar yechimni kiritish jarayonini avtomatlashtirish imkonini beradi.

3.7. Axborot xavfsizligi insidentlarini boshqarish dasturlari

Axborot xavfsizligi insidentlarini boshqarish dasturlarining asosiy vazifasi AXI hujjatlarni to'liq yaratilish, AXI qayta ishlash jarayoni va ketma-ketligini tavsiflab berishi hvmda AXI haqida xabardor etish vazifalarini bajarishi karak. Axborot xavfsizligi insidentlarini boshqarish dasturlari AXI hodisalariga tegishli harakatlarini aniqlashi kerak bo'ladi. Axborot xavfsizligi insidentlarini boshqarish dasturlarining qo'llanilishi:

- axborot xavfsizligi insidentlariga javob qaytarish;
- insident aniqlanishi, niqlangan insidentni bartaraf etish yoki AXI sfatida qabo'l qilishi;
- axborot xavfsizligi insidentlarini rexsat berilguncha boshqarish;
- identifikasiya qilinib aniqlangan insidentlarini qayta ishlash, har ehtimolga qarshi xavfsizlik tizimini takomillashtirish;
- identifikasiyalashni amalga oshirishni yaxshilash.

Axborot xavfsizligi insidentni tahlillashni apparat va dasturiy ta'minoti:

- kompyuter jinoyatchiligi ish stansiyalari yoki zaxira qurilmalar, noutbuklar;
- maxsus (server ish stansiyalari va tarmoq) qurilmalar;
- bo'sh ma'lumot tashuvchi qurilmalar, kabellar, binolar, o'zgartgichlar va yozish huquqini cheklash;
- kichgina printer;
- tarmoq protokoli va paketlarni snifferlash tahlillagichlari;
- kompyuter jinoyatchiligini dasturiy taminoti;
- ma'lumot saqlovchi qurilmalar;
- dalillarni yig'ishdagi (misol, noutbuklar, kameralar, yozib oluvchi qurilmalar, dalillar yig'ilgan fayllar papkasi) ruxsatlar.

Texnik va boshqa yordam (shu jumladan operasion yordam)

Axborot xavfsizligi insidentlariga tez va samarali javob berilishini ta'minlash uchun tashkilot kerakli texnik va boshqa yordam vositalarini sotib olishi, tayyorlashi va tekshirishi lozim. Bularga quyidagilar kiradi:

a) tashkilot aktivlarining tavsifi, shu jumladan, aktivlarning yangilangan ruyxati va ularning biznes-funksiyalar bilan aloqalari haqidagi ma'lumotlardan foydalanish imkoni;

b) krizisga qarshi boshqarish bilan bog'liq hujjatlashtirilgan proseduralarni ishlatish imkoniyati;

c) axborot uzatishning hujjatlashtirilgan va e'lon qilingan jarayonlari;

d) axborot xavfsizligi hodisalari/insidentlari/zaifliklari ma'lumotlar omborini va texnik vositalarni ma'lumotlar omborini tez to'ldirish va yangilash, undagi axborotni tahlil qilish va javob berish jarayonlarini soddalashtirish uchun qo'llash (ayrim xollarda tashkilotga qo'lda qilingan yozuvlar kerak bo'lishi mumkin); ma'lumotlar omborini ishonchli saqlash;

e) axborot xavfsizligi ekspert dalillarini yig'ish va tahlil qilish uchun uskunalar;

f) axborot xavfsizligi zaifliklari hodisalari/insidentlari/ zaifliklari ma'lumotlar omborini krizisga qarshi boshqarishning mutanosib choralari.

Tashkilot ma'lumotlar omborini tez kiritish va yangilash uchun ishlatiladigan texnik vositalar tomonidan axborotni tahlil qilish va axborot xavfsizligi insidentlariga javob jarayonini yengillashtirishni hamda ularning quyidagilarda yordam berishini taminlash lozim:

a) axborot xavfsizligi hodisalari/insidentlari/zaifliklari haqidagi hisobotlarni tez olish;

b) tegishli oldindan tanlangan uchinchi shaxslarning bu maqsad uchun tanlangan vositalar (masalan, elektron pochta, faks va telefon) orqali hisobot berishi, ya'ni qulay va qog'ozdagi va boshqa nushalarni o'z ichiga olgan hamda ma'lumotni xavfsiz usul bilan (zarurat bo'lganda) uzatish imkoniyatlariga ega bo'lgan ishonchli kontakt ma'lumotlar omborining yordamini so'rash orqali;

c) tizim, xizmat va/yoki tarmoqqa hujum paytida Internet yoki boshqa vosita orqali joriy qilinadigan elektron aloqaning ishlashini ta'minlaydigan, baholangan tahdidlarga mos ehtiyot choralarining ko'rilishi (buning uchun oldindan tayyorlangan muqobil aloqa vositalarini qo'llash kerak bo'lishi mumkin);

d) axborot tizimi, xizmati va/yoki tarmog'i hamda barcha qayta ishlanayotgan ma'lumotlar haqidagi barcha ma'lumotlarni yig'ish jarayoni;

e) o'zgarishlar mavjudligini hamda tizim, xizmat va/yoki tarmoqning qaysi qismlari va qaysi ma'lumotlar o'zgartirilganini aniqlashga yordam berish maqsadida butunlikni kriptografik nazorat qilish usulini ishlatish, agar bu baholangan tahdidlarga mos kelsa;

f) yig'ilgan axborotni arxivlash va himoya qilishni soddalashtirish (masalan, faqat CD yoki DVD ROM qurilmalarida o'qish uchun mo'ljallangan tashuvchilarga avtonom ravishda saqlashdan oldin qayd jurnallarida raqamli imzo yoki boshqa yozuvlarni qo'llash orqali);

g) axborot xavfsizligi insidentini bartaraf qilish jarayonini aks ettiruvchi va axborotning butunligini ta'minlovchi hujjatlarni (masalan, qayd jurnallarini) chop etishga tayyorlash;

h) krizisga qarshi boshqarishga muvofiq ravishda quyidagi proseduralar orqali axborot tizimi, xizmati va/yoki tarmog'ining odatiy ish rejimini tiklash:

- rezerv nushalarini sinovdan o'tkazish;
- zararli dasturlarni nazorat qilish;
- tizimli va amaliy dasturiy ta'minotga ega asl axborot tashuvchilaridan foydalanish;
- yuklovchi axborot tashuvchilarni qo'llash;
- tizimli dasturiy ta'minot va ilovalarning toza, ishonchli yangilanishlarini qo'llash.

Tashkilotlar orasida o'rnatuvchi diskdan standart bazaviy obraz yaratish va bu obrazni tizim yaratishning toza asosi sifatida qo'llash keng tarqalmoqda. Bunday obrazning original manbaa o'rniga ishlatilishi ko'pincha maqsadga muvofiq, chunki obraz o'zgartirilgan, tasdiqlangan, sinalgan va hokazo.

Hujumga uchragan axborot tizimi, xizmati va/yoki tarmog'i noto'g'ri faoliyat ko'rsatishi mumkin. Shuning uchun axborot xavfsizligi insidentiga javob berish uchun kerakli texnik vositalarning (dasturiy yoki apparat ta'minoti) ishi tashkilotda ishlatiladigan tizimlar, xizmatlar va/yoki tarmoqlarga asoslanmasligi lozim. Iloji boricha hodisaga javob berishning texnik vositalari to'liq avtonom bo'lishi kerak.

Izoh - Ushbu punkda ko'rsatilgan texnik vositalarga bevosita axborot xavfsizligi insidentlari va xujumlarini aniqlash, shuningdek, tegishli shaxslarni avtomatik ogoh qilishda ishlatildagigan texnik vositalar kirmaydi.

Kontakt posiziyasi (KP) tashkilotning axborot texnologiyalari va tegishli axborotni qayta ishlash bilan bog'liq barcha aspektlarini

qo'llab-quvvatlashda keng qamrovda qo'llanilsa ham, axborot xavfsizligi insidentlarini boshqarishda muhim rol o'ynaydi. Agar axborot xavfsizligi voqealari haqida birinchi marta xabar berilayotgan bo'lsa, KP ular bilan aniqlash va hisobot bosqichida ko'rishadi. KPda yig'ilgan ma'lumotni qayta ko'rib chiqish va hodisani insident sifatida tasniflash lozimligiga dastlabki baho berish lozim. Agar hodisa insident sifatida tasniflanadigan bo'lsa, KP u bilan kurashadi, lekin aksar xollarda insidentni bartaraf qilishga axborot xavfsizligi insidentlariga ta'sir etish xizmati mas'ul bo'lishi lozim. KP xodimlari xavfsizlik bo'yicha ekspertlar bo'lishlari maqsadga muvofiq.

Boshqarish sxemasini testdan o'tkazish

Axborot xavfsizligi hodisalari va insidentlarini boshqarish jarayonida yuzaga kelishi mumkin bo'lgan ehtimoliy kamchiliklar va muammolarning oldini olish uchun tashkilot axborot xavfsizligi insidentlarini boshqarish jarayonlari va proseduralarini muntazam tekshirish va nazoratdan o'tkazishni rejalashtirishi lozim. Axborot xavfsizligi insidentiga javobni tahlil qilish natijasida yuzaga keladigan har qanday o'zgarishlar jiddiy tekshiruv na nazoratdan o'tishi lozim. Tashkilot test proseduralarining tahlili natijasida kiritilgan har qanday o'zgarishlarning batafsil tekshirilishini, shuningdek, o'zgargan boshqarish sxemasi ishga tushishidan oldin keyingi tekshiruvni kafolatlashi lozim.

Axborot xavfsizligi insidentlarini boshqarish dasturlariga amalga oshiriladigan hujumlar

1. Xizmat ko'rsatishda rad etish

Xizmat ko'rsatishda rad etish (DoS) va xizmat ko'rsatishda taqsimlangan rad etish (DDoS) - umumiy yo'nalishga ega bo'lgan insidentlarning yirik kategoriyalari. Bunday insidentlar tizim, xizmat yoki tarmoqning ishi uning imkoniyatlari to'liq hajmida to'xtab qolishiga sabab bo'ladi va odatda mualliflashgan foydalanuvchilarning ham xizmatdan foydalanishini to'liq rad qiladi. Texnik vositalar bilan bog'liq DoS/DDoS insidentlarining ikki asosiy turi mavjud: manbaaning yo'q qilinishi va manbaaning osilib qolishi.

Ataylab uyushtirilgan DoS/DDoS texnik insidentlarining ayrim tipik namunalari:

- tarmoq diapazonini javob trafiki bilan to'ldirish maqsadida tarmoq uzatishini ping-so'rovlar yordamida tekshirish;

- tizim, xizmat yoki tarmoqni barbod qilish yoki uning normal ishlashini to'xtatish maqsadida unga noma'lum formatda ma'lumotlar yuborish;

- konkret tizim, xizmat yoki tarmoqning resurslarini tugatish (ya'ni sekinlashtirish, yoqish yoki ularni ishlatishni rad etish) maqsadida u bilan ruxsat etilgan sessiyalar tarmog'ini ochish.

Bunday hujumlar ko'pincha bot-tarmoqlar - avtonom va avtomatik boshqariladigan dasturiy robotlar (zararli kodlar) orqali amalga oshiriladi. Bot-tarmoqlar yuzlab, millionlab zararlangan kompyuterlarga aloqador bo'lishi mumkin.

Ayrim texnik DoS insidentlari tasodifan, masalan, operatorning noto'g'ri konfigurasiyasi yoki dasturiy ta'minotning mos kelmasligi tufayli yuzaga kelgan bo'lishi mumkin, lekin aksar hollarda ular ataylab uyushtirilgan bo'ladi. Ayrim texnik DoS insidentlari ataylab tizim yoki xizmatni barbod qilish, tarmoqni yopish maqsadida uyushtiriladi, boshqalari esa boshqa zararli faoliyatning natijasi bo'lishi mumkin. Masalan, ayrim identifikasiya va skanerlash usullari skanerlash paytida eski tizimlar yoki noto'g'ri konfigurasiyali tizimlarning barbod bo'lishiga olib kelishi mumkin. Shuni qayd etish lozimki, ko'pincha texnik DoS insidentlari anonim tarzda ishga tushiriladi (ya'ni hujum manbai sohtalashtirilgan bo'ladi).

Texnik vositalar sababli yuzaga kelgan va axborot, xizmat va/yoki vositalarning yo'qotilishi bilan tugaydigan DoS insidentlariga quyidagilar misol bo'la oladi:

- qurilmaning o'g'irlanishi, unga ataylab zarar yetkazilishi yoki uning ishdan chiqarilishi bilan tugaydigan jismoniy xavfsizlik choralarining buzilishi;

- yong'in yoki suv toshqini natijasida apparat vositalari (va/yoki ular joylashgan joy)ga tasodifan zarar yetishi;

- atrof muhitning favqulodda holatlari, masalan, ish sharoitining yuqori harorati (kondisionerning ishdan chiqishi natijasida);

- sistemadagi uzilishlar yoki o'chirib qayta yoqishlar;

- tizimning nazorat qilinmagan o'zgarishlari;

- dasturiy ta'minot yoki apparat vositalaridagi uzilishlar.

2. Ruxsatsiz foydalanish

Umuman olganda, insidentlarning bu guruhi tizim, xizmat yoki tarmoqdan ruxsatsiz foydalanishga urinishdan iborat. Texnik ruxsatsiz foydalanish insidentlariga ayrim misollar:

- parollar fayllarini tiklashga urinish;

- obyektdan to'liq (masalan, tarmoq ma'muri darajasida) foydalana olish imkoniyatini qo'lga kiritish uchun almashinuv buferini to'ldirish hujumi;

- resurslar yoki ma'lumotga foydalanuvchi yoki administrator qonuniy asoslarda ega bo'lgan foydalanish imkoniyatidan ko'ra ko'proq darajada foydalanish imkonini qo'lga kiritishga urinishlar.

Texnik bo'lmagan vositalar yordamida ma'lumotni bevosita yoki bilvosita oshkor qilish yoki o'zgartirish, bo'ysunishning buzilishi yoki axborot tizimlarini noto'g'ri ishlatish natijasida yuzaga kelgan ruxsatsiz foydalanish insidentlariga quyidagilar sabab bo'lishi mumkin:

- axborotdan ruxsatsiz foydalanish natijasida jismoniy xavfsizlik choralarining buzilishi;

- tizimdagi nazorat qilinmagan o'zgarishlar yoki dasturiy yoki apparat ta'minotidagi uzilishlar natijasida operasion tizimning yomon va/yoki noto'g'ri sozlanishi.

3. Zararli kodlar

Zararli kod - bu boshqa dasturga uning dastlabki harakat modelini o'zgartirish va odatda zararli faoliyat turlarini amalga oshirish, masalan, ma'lumotlar va shaxsiy ma'lumotlarini o'g'irlash, axborot va resurslarni yo'q qilish, xizmat ko'rsatishni rad etish, spam tarqatish va hokazolar maqsadida kiritilgan dastur yoki dasturning bir qismi. Zararli dasturning hujumlarini besh turkumga bo'lish mumkin: viruslar, qurtlar, "troyan dasturlari", mobil kodlar va aralash dasturlar. Bir necha yillar oldin viruslar zararlangan zaif muhit yaratish maqsadida yozilgan bo'lsa, bugungi kunda zararli kodlar maqsadli hujumlarni amalga oshirish uchun ishlatiladi. Bu mavjud zararli kodni o'zgartirish, zararli kodni aniqlash texnologiyalari tomonidan aniqlanmaydigan prototiplarni yaratish orqali amalga oshiriladi.

4. Nomaqbul foydalanish

Bunday insident foydalanuvchi tashkilot axborot tizimini xavfsizlik siyosatini buzganda yuz beradi. Bunday insidentlar aslida hujum hisoblanmaydi, lekin ko'pincha insident sifatida xabar beriladi va AXITX nazorati ostida bo'lishi lozim. Quyidagilar nomaqbul foydalanishga misol bo'lishi mumkin:

- buzish uchun dasturlarni yuklash va o'rnatish;

- korporativ elektron pochta qutisidan spam tarqatish yoki shaxsiy biznesini ilgari surish maqsadida foydalanish;

- korporativ resurlardan ruxsat berilmagan veb-saytni sozlash maqsadida foydalanish;

- markazlashmagan tarmoqdan qaroqchi fayllarni (musiqa, video, dasturiy ta'minot) olish yoki tarqatish maqsadida foydalanish.

Asosiy xulosalar

AX hodisalarini aniqlashni, ular bilan bog'liq axborotni umumlashtirishni va ularning yuzaga kelishi va zaifliklar mavjudligi yuzasidan qo'l yoki avtomatlashtirilgan vositalar yordamida tayyorlangan hisobotlarni o'z ichiga oladi.

Har bir tadbir davomida hisobotda ko'rsatilgan axborot ayni paytda imkon qadar to'liq bo'lishi shart, bu unga tegishli baho berilishiga, tegishli qaror qabul qilinishi va ish-harakatlar amalga oshirilishiga olib keladi.

Ichki insident – zarar ko'rgan tomon bilan bevosita (mehnat shartnomasi) bog'liq bo'lgan shaxs tomonidan amalga oshirilgan insident.

Tashqi insident – bu zarar ko'rgan tomon bilan hech qanday bog'liqligi bo'lmagan shaxslar tomonidan uyushtirilgan insident.

Hisobotlarni soxtalashtirish - bu bilib turib ma'lum bir harakatlardan keyin ma'lumotlarni noto'g'ri aks ettirish.

SIEM (Security information and event management) – AXni boshqarish va xavfsizlik hodisalarini nazorat etish.

Istalgan jarayonni boshqarishda shu jarayonning qiyin nuqtalari mavjud bo'ladi. Ushbu muammolarni hal qilish esa ishning qanchalik unumdor bo'lishini aniqlab beradi.

Insidentlarni boshqarishning asosiy vositalariga monitoring tizimi va xodisalarining axborot xavfsizligi korrelyasiyasi xisoblanadi, tahlil natijalari asosida aks ta'sir strategiyasi ishlab chiqiladi.

Insidentni anomalligi to'g'risidagi xulosa har tomonlama tahlil qilish uchun asos bo'ladi. Shularni hisobga olgan holda presedentli tahlil insidentlarni normal va normal bo'lmagan sinflarga ajratishni nazarda tutadi.

Presedentli analiz konsepsiyasini vosita sifatida qo'llash, axborot xavfsizligi insidentlarini boshqarish jarayonini takomillashtish, insidentlarga nisbatan aks ta'sir operativligini orttirilgan tajribani qo'llash orqali bir necha marta oshiradi. Undan tashqari, bunday yondoshuv har tomonlama o'rganilishi dolzarb bo'lgan anomal insidentlarni aniqlash masalasini hal qiladi.

Nazorat uchun savollar.

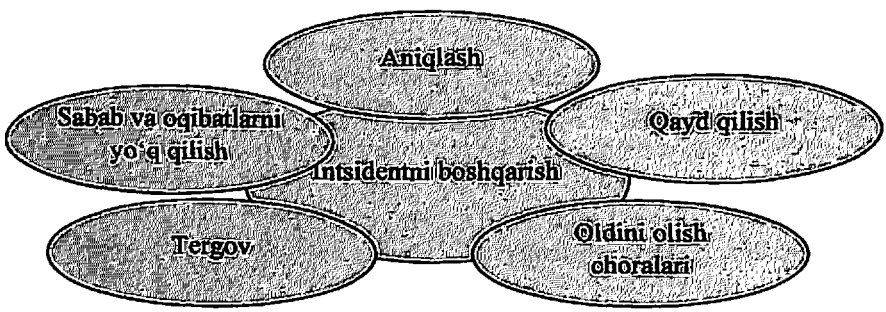
1. Axborot xavfsizligi insidentlari va hodisalari to‘g‘risidagi hisobot deganda nimani tushunasiz?
2. Axborot xavfsizligi insidentlari va hodisalari qayta ishlash jarayonini tushuntiring.
3. Ichki insident nima?
4. Tashqi insident nima?
5. Axborot xavfsizligi insidentlarini guruhlarga ajratish ketma ketligini tushuntirib bering.
6. Hisobotlarni soxtalashtirish qanday amalga oshiriladi?
7. Aktivlarni o‘g‘irlash (moliyaviy yoki material) nimani anglatadi?
8. Sobataj nima?
9. Lavozimdan yovuz maqsadlarda foydalanish qanday usullari bo‘lishi mumkin?
10. UZ-CERT va RU-CERTning bir biridan farqi nimada?
11. SIEM nima?
12. Testlash va takomillashtirish jarayonlarining o‘zaro bog’liqligi nimada?
13. Axborot xavfsizligi insidentlarini boshqarishda yuzaga keladigan muammolar.
14. Presedentli taxlilni qo‘llash konsepsiyasi tushuntirib bering.
15. Presedentli taxlil tizimi arxitekturasi qanday ishlab chiqilgan.
16. Axborot xavfsizligi insidentlarini boshqarish dasturlarini sanab ko‘rsating va ularning bir biridan asosiy farqini tushuntiring.

4. AXBOROT XAVFSIZLIGI INSIDENTLARINI TADQIQ QILISH

4.1. Insidentlarni tadqiq qilish bosqichlari

Tashkilot va firmalarda insidentlarni aniqlashning usuli yo'q, va xodimlar qanday hodisalar insidentlar bo'lishi mumkinligi haqida ma'lumotga ega emaslar. Bu, ayniqsa, axborot xavfsizligi insidentlarida katta ahamiyatga ega - negaki ular har doim ham normal ish tartibini buzmaydi. Masalan, xavfsizlik insidentiga stolda maxfiy hujjatlarni qoldirishni kiritish mumkin. Buni hech kim e'tiborga olmaydi va tajovuzkor (kompaniya xodimi bo'liishi mumkin) bunday hujjatlarni ko'radi. Insidentlarning tadqiq qilish bosqichida quyidagilar asosiy rolni o'ynaydi: insident qaydlari mavjud jurnallarni saqlash, foydalanuvchi vakolatini aniq ajratish, bajarilgan harakatlar uchun javobgarlik – hodisada kim ishtirok etgan va qanday harakatlar qilganini ko'rsatadigan dalillar muhimdir. Insidentlarning oqibatlari bartaraf etilgach va biznes-jarayonlar qayta tiklangach, insidentni tekshirish, tuzatuvchi va profilaktika choralarini amalga oshirish uchun hech qanday choralar ko'rilmaydi.

Insident - xizmatning standart operatsiyalari tarkibiga kirmagan, xizmat ko'rsatishning to'xtalishi yoki xizmat sifatining yomonlashishiga sabab bo'lishi mumkin bo'lgan har qanday hodisadir (4.1- rasm).



4.1- rasm. Axborot xavfsizligi insidenti

Insidentlarni tadqiq qilish bir qancha asosiy maqsadlar ifodalaydi:

- axborot havfsizligi insidentlarining oqibatlarini lokalizatsiya qilish va tugatish;
- jinoyatchilarni va ularning motivatsiyalarini aniqlash, ularni javobgarlikka tortish imkoniyatlarini ta'minlash;

- insidentlar tahlili va kelgusida ham shunga o'xshash holatlarning oldini olish choralarini ko'rish.

- Boshqa xususiy maqsadlar muayyan hodisaning aniq tergovi orqali amalga oshirilishi mumkin. Tekshiruvning yagona metodologiyasi yo'q, lekin umuman tergov davomida quyidagi harakatlar amalga oshiriladi:

- dalillarni to'plash va tahlil qilish;

- jinoyatchilarni aniqlash va ularni javobgarlikka tortish choralarini ko'rish;

- insidentning sabablarini aniqlash;

- insidentlarning oldini olish bo'yicha choralar ko'rish uchun tavsiyalar berish;

- tadqiq materiallarini saqlash va himoya qilish.

Ba'zi muhim bosqichlarni ko'rib chiqamiz.

Axborot xavfsizligi insidenti bo'yicha dalillar yig'ish - tadqiq jarayonning eng muhim qismidir, qanday maqsadda amalga oshirilishidan qat'iy nazar. Uning muvaffaqiyati asosan to'plangan dalillarning sifatiga bog'liq, shuning uchun dalillar qator majburiy talablarga javob berishi kerak:

- to'liqligi (hodisani obektiv o'rganish uchun dalil yetarli);

- ahamiyati (dalil insidentga bog'liq);

- aniqligi (dalillar ishonchli manbalardan olingan va o'zgartirilmagan);

- ruxsat etilganligi (dalillar qonuniy yo'l bilan olinishi kerak).

Tadqiqning dastlabki bosqichida, dalillarning sudda qo'l kelishi mumkinmi yoki yo'q, aytish qiyin (chunki, hodisaning tabiati, aybdor va uning niyatlari hali noma'lum), shuning uchun ruxsat etilganlik, aniqlik va to'liqlik talablariga jiddiy e'tibor qaratish, "iblis mayda narsalarda yashirinadi" prinsipi bo'yicha ish ko'rish lozim. Bundan tashqari, jinoyat ishi bo'yicha tergovchi yoki tezkor vakil xodimi tomonidan amalga oshirilishi mumkinligini yodda tutish kerak, agar zarur bo'lsa, huquqni muhofaza qilish organlari bilan tezkor aloqa qilish kerak.

Insidentlarni, virus tarqalishini tadqiq qilishning asosiy maqsadi hujumning oqibatlarini, uning kelib chiqish sabablari va usullarini aniqlashdir. Hujumning sabablari va usullarini aniqlash orqali takrorlangan hujumlar va infeksiyalarning oldini olish uchun tuzatuvchi harakatlar qilish mumkin. Axborot xavfsizligi bo'yicha mutaxassislarning tajribasi shuni ko'rsatadiki, hujumga uchragan yoki

viruslangan tashkilot insidentning chegaralarini har doim ham to‘g‘ri aniqlay olmaydi va shuning uchun oqibatlarni baholash va bartaraf etishning iloji yo‘q. Hozirgi kunda hujum va virus tarqalish oqibatlarini bartaraf etish bo‘yicha umumiy tavsiyalar mavjud emas.

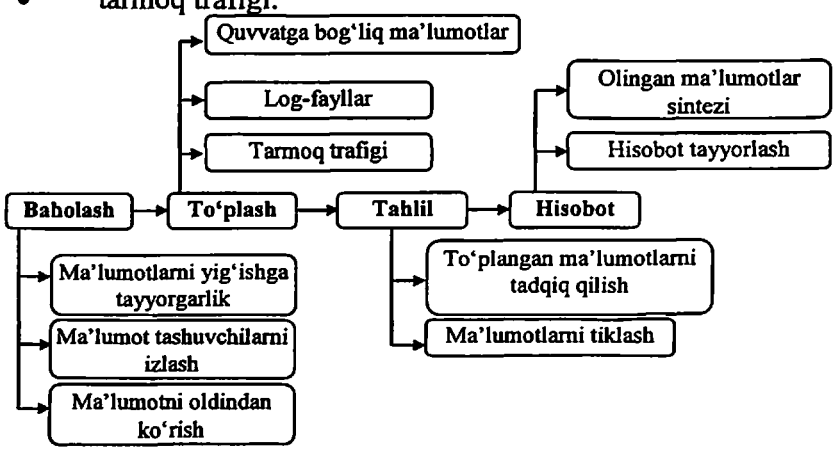
Insidentlarni tadqiq qilish xavfsizlik sohasidagi muhim vazifalardan biri hisoblanadi. Avval axborot xavfsizligi insidentlarini tadqiq jarayonini batafsil ko‘rib chiqamiz. Umuman olganda, u quyidagi ko‘rinishda bo‘ladi (4.2- rasm):

1-Bosqich. Baholash. Ushbu bosqichda axborot xavfsizligi insidenti bilan bog‘liq ma’lumotlarni to‘plash bo‘yicha tayyorgarlik ishlari olib boriladi, ya’ni tadqiq qilish imkoniyatlari ko‘rib chiqiladi (tadqiq qilish uchun ruxsat olinadi, amaldagi havfsizlik siyosati va qonunlar tahlil qilinadi); tadqiq o‘tkazadigan guruh tarkibi belgilanadi; hodisa yuz bergan tarmoq topologiyasi o‘rganiladi; kriminalistikaga ta’luqli ma’lumotlarning manbalari aniqlanadi va hokazo.

Bundan tashqari, baholash bosqichida hodisa bilan bog‘liq bo‘lgan kompyuterni saqlash vositasi aniqlanadi.

2-bosqich. To‘plash. Ushbu bosqichda insident bilan bog‘liq barcha ma’lumotlar yig‘iladi. Ular quyidagilardir:

- quvvatga bog‘liq bo‘lmagan axborot vositalarining tarkibi (qattiq disklar, ixcham disklar, USB flesh-disklar va h.k.);
- quvvatga bog‘liq ommaviy axborot tashuvchilar tarkibi (tezkor xotira);
- tarmoq uskunalari, serverlarning log-fayllari;
- tarmoq trafigi.



4.2- rasm. Axborot xavfsizligi insidentlarini tadqiq qilish jarayonlari

Quydagi ma'lumotlarni to'plash maxsus asboblar bilan nusxasini yaratishdan iborat.

Quvvatga bog'liq bo'lmagan axborot vositalarining tarkibi. Quvvatga bog'liq bo'lmagan vositaning nusxasini yaratmasdan oldin, dasturiy ta'minot va apparatni ro'yxatga olish blokirovkalari ishlatiladigan kontentning yaxlitligi (o'zgarmasligi), shuningdek, maxsus operatsion tizimlarni ta'minlash kerak. Nusxa ko'chirish (yoki o'chirish) kerak bo'lgan kompyuter ishlayotgan bo'lsa, unda quvvatga bog'liq bo'lmagan ma'lumotlar yig'ilgandan so'ng kompyuter faoliyati to'xtaydi, quvvatga bog'liq bo'lmagan ma'lumot yig'ilmasligi kerak bo'lsa darhol to'xtatiladi; maxsus holatlarda (masalan, o'ta muhim serverlarni o'chirib qo'yish imkoni bo'lmaganda), ishlaydigan tizimdan quvvatga bog'liq bo'lmagan ma'lumotlarning nusxasini ko'chirish mumkin.

Yozuv blokirovkalari operatsion tizimning yoki uchinchi tomon dasturlarining xatosidan kelib chiqadigan xato tufayli ma'lumotni yozish xavfsiz ma'lumotlar tashuvchisini ulash imkonini beradi.

Uskuna blokatorlari ushbu ma'lumotlarni o'qish uchun ishlatiladigan operatsion tizimlar va dasturlardan qat'iy nazar o'z vazifalarini bajaradilar. Ixtisoslashgan operatsion tizimlar, qoida tariqasida, tadqiq qilish ostida bo'lgan kompyuterdan ishonchli (kriminalistik) dasturiy ta'minot muhiti o'rnatilishi orqali ma'lumot tashuvchi vositalarni nusxalash uchun ishlatiladi. Odatda, ushbu operatsion tizimlar CD yoki USB Flash vositasidan yuklanadi va yuklash jarayonida dasturiy yozuvlarni blokirovkalashni o'z ichiga oladi. Bunday operatsion tizimlarning namunalari:

- grml;
- CAINE Live CD;
- DEFT Linux;
- e-fense Helix3 Pro.

Quyidagi dasturlar to'g'ridan-to'g'ri ma'lumotlarni ko'chirib olish uchun ishlatilishi mumkin:

- dd (deyarli barcha Linux tarqatuvchilari tarkibiga kiradi);
- dc3dd - dd ning o'zgartirilgan versiyasi;
- aimage;
- FTK Imager.

O'rganishdan oldin quvvatga bog'liq bo'lmagan ma'lumotlarni tashuvchi vositalarning tarkibidan nusxa ko'chirish ixtiyoriy ekanini

ta'kidlash lozim - vositaning asl tarkib yaxlitligi saqlangan hollarda (masalan, vositaning sozligi yoki yozuvni bloklash qo'llanilganda), aslning o'rniga nusxalarini o'rganish maqbul emas.

Quvvatga bog'liq ma'lumotlarni to'plash operatsion tizimlardan ularni o'chirishdan oldin amalga oshiriladi. Odatda, quvvatga bog'liq ma'lumotlarni yig'ish jarayoni quyidagilardan nusxa olishdan iborat:

- kompyuterning tezkor xotira tarkibi;
- o'rnatilgan shifrlangan fayllar va tarmoq omborlari tarkibi;
- faoliyat yuruvchi jarayonlar va xizmatlar ro'yxati;
- joriy tarmoq ulanishlar va ochiq portlar ro'yxati;
- o'rganilayotgan tizimning tarmoq konfiguratsiyasi;
- muhit o'zgaruvchilari;
- monitor ekranida foydalanuvchi ko'rgan tasvir (ekran tasvirini yaratish).

Ushbu ma'lumotni o'rganilayotgan operatsion tizimga nusxalash uchun tashqi ma'lumot tashish vositalari ulanishi mumkin, undan ma'lumotlarni to'playdigan maxsus dastur ishga tushiriladi. Ba'zan tarmoq orqali tizimga maxsus dastur yuklanadi. Nusxalangan ma'lumotlar tashqi muhitda saqlanishi yoki tarmoq orqali ishonchli serverga uzatilishi mumkin.

Loglarni nusxalash bir necha usulda amalga oshirilishi mumkin:

- faqat muayyan insidentga bog'liq ma'lumotlarga oid yozuvlarni ko'chirib olish (masalan, muayyan bir IP-manzil yoki vaqt oralig'iga bog'liq);
- log fayllardan butunlay nusxa ko'chirish;
- barcha axborot tashuvchilarini nusxalash.

U yoki bu nusxa ko'chirish usulini tanlashda asosiy omillar quyidagilardir: loglarga bo'lgan ishonch darajasi va shunga muvofiq, loglarining to'g'riligi va o'zgarmasligi darajasini aniqlashga yo'naltirilgan tadqiqot miqdori. Log fayllarning zararli o'zgarishi yoki soxtalashtirilishi ehtimoli kichkina bo'lsa, faqat log fayllarni yoki ularning alohida yozuvlarini ko'chirib olish joizdir. Aks holda, butun tashuvchi vositasining tarkibini (tizimga ruxsatsiz kirish izlarini, log fayllarini o'zgartirish izlari va boshqalarni qidirib topish uchun) nusxalash tavsiya etiladi.

3-bosqich. Tahlil. Ushbu bosqichda yig'ilgan ma'lumotlarning tahlili quyidagi algoritmga muvofiq amalga oshirilishi mumkin:

– obekt (disk, diskning nusxasi, tarmoq trafigi dampi va boshqalar) haqida umumiy ma'lumot olish;

– ma'lumotlarni ochiq holatda o'rganish;

– bilvosita (masofadan, yashirin, shifrlangan) shaklda ma'lumotlarni o'rganish.

Quvvatga bog'liq bo'lmagan ma'lumot tashuvchi vositalarni va ularning nusxalarini o'rganish ko'p hollarda fayl tizimlarining tarkibini o'rganish va ma'lumotlarni tiklashdan iborat. Fayl tizimlarini tadqiq qilish tajovuzkorning harakatlaridan kelib chiqadigan turli xil axborot izlarini tahlil qilish, tergov qilinayotgan tizimning dasturiy ta'minotini va uskunasini tahlil qilishdan iborat. Fayl tizimlarida ushbu izlarning soni (kriminaltstik ahamiyatga ega ma'lumotlar manbai sifatida) juda katta bo'lib, shuning uchun insidentlarni tekshirishda fayllar tizimini kriminaltstik tadqiq qilish uchun keng qamrovli usullar va algoritmlar mavjud emas.

Fayl tizimlarini kriminaltstik tadqiq qilish uchun quyidagi dasturiy mahsulotlardan foydalanish mumkin:

– EnCase Forensic;

– Forensic Toolkit;

– The Sleuth Kit.

Quyidagi dasturlar ma'lumotlar uzatish uchun ishlatilishi mumkin:

– Foremost;

– PhotoRec.

Tarmoqli paketlar dampining tahlillari quyidagicha:

– tarmoq paketlari va ulanishlarining xususiyatlarini aniqlash (masalan, maxfiy ma'lumotlarni qidirish uchun);

– tarmoq orqali uzatiladigan xabarlarni chiqarish (masalan, axborot tarqalish kanallarini qidirish uchun).

Birinchi holda tarmoq paketlarini analizatorlari quyidagilar qo'llanilishi mumkin:

– Wireshark;

– Network Miner.

Ikkinchi holatda, odatda, tarmoq paketlarini tahlil qiladigan mutaxassislar emas, balki turli xil tarmoq xabarlarini (elektron pochta xabarlari, internet peygerlar, va hokazo) izlash, chiqarish va saqlash jarayonlarini avtomatlashtirishga imkon beruvchi yuridik qo'lga olish tizimlari, shuningdek, kalit so'zlar va qo'lga olinuvchi ma'lumotlarning boshqa mezonlarini kiritishdan foydalaniladi.

4-bosqich. Hisobot. Ushbu bosqichda tahlil qilish bosqichida olingan barcha ma'lumotlarning sintezi, so'ngra hisobotni u mo'ljallangan auditoriya uchun tushunarli bo'lgan shaklda yozish amalga oshiriladi. Hisobot quyidagilarni o'z ichiga olishi mumkin:

- insident sabablari haqida ma'lumotlar;
- insidentga aloqador shaxslar to'g'risidagi ma'lumotlar;
- insident xronologiyasi;
- tahlil davomida aniqlangan izlar (dalil) ning batafsil tavsifi;
- jarayon davomida qo'llanilgan tadqiq qilish usullari, dasturiy va apparat ta'minot, ularni qo'llash holatlari haqida ma'lumot;
- kelajakda shunga o'xshash insidentlarni oldini olish uchun tavsiyalar.

Insident haqida xabardor etish. Avvalo insident haqida ma'lumot olish kerak. Bu haqida xavfsizlik siyosatini shakllantirish va xodimlar uchun axborot xavfsizligida ta'lim bo'yicha prezentatsiyalar yaratish bosqichida o'ylash zarur.

Axborotning asosiy manbalari:

1. ***Helpdesk.*** Odatda qurilmadagi har qanday nosozlik AT-servisning yordam paneliga yoziladi yoki telefon orqali xabar beriladi. Shuning uchun, "xelpdesk" ish jarayoniga oldindan "integratsiya qilinish" va talabnomaning axborot xavfsizligi bo'limiga o'tkazilishi kerak bo'lgan insidentlar turlarini ko'rsatish kerak.

2. ***Foydalanuvchilardan bevosita xabarlar.*** Bitta aloqa nuqtasini tashkil qiling va bu haqda havfsizlik xodimlari uchun treningda xabar bering. Hozirgi kunda tashkilotlarda axborot xavfsizligi bo'linmalari odatda juda katta emas, ko'pincha 1-2 kishidan iborat. Shuning uchun u insidentlar uchun javobgarni tayinlash qiyin bo'lmaydi, IS Helpdesk ehtiyojlariga ko'ra elektron pochta manzillarini aniqlashtirish bilan ovora bo'lishning keragi yo'q.

3. ***Xavfsizlik xodimlari tomonidan topilgan insidentlar.*** Bunda har bir narsa oddiy va bunday qabul qilish kanalini tashkil qilish uchun hech qanday imo-ishora talab qilinmaydi.

4. ***Loglar va ogohlantirish tizimlari.*** Antivirus, IDS, DLP va boshqa xavfsizlik tizimlarining konsolida ogohlantirishlarni sozlang. Tashkilotda o'rnatilgan dastur va tizimlar loglaridan ma'lumotlarni to'playdigan agregatorlardan foydalanish ancha qulaydir. Tashqi tarmoq bilan aloqador nuqtalarga va sezgir axborotni saqlash joylariga alohida e'tibor berilishi kerak.

4.2. Insidentni toifalash va klassifikatsiyasi

Garchi xavfsizlik insidentlari xilma-xil bo'lsa-da, ular statistikani saqlash osonroq bo'lgan bir necha toifaga bo'linadi.

*1. **Maxfiy yoki ichki axborotni oshkor qilish yoki bunday oshkor qilishga tahdid.*** Buning uchun, eng kamida, maxfiy axborotning hozirgi ro'yxatini, elektron va qog'oz axborot vositalarini belgilashning faoliyat yurituvchi tizimiga ega bo'lish kerak. Yaxshi misol - korxona ichki portalida yoki ichki fayllarni saqlash muhitida joylashgan deyarli barcha hayotiy vaziyatlar uchun yaratilgan hujjat andozalari odatiy ravishda "Faqat ichki foydalanish uchun" deb belgilanadi.

*2. **Ruxsatsiz kirish.*** Buning uchun himoyalangan resurslar ro'yxatini kiritish kerak. Boshqacha aytganda, tashkilotning, mijozlarning yoki pudratchilarning ma'lumotlari qayerda saqlanishini bilish lozim. Bundan tashqari, bu toifaga nafaqat kompyuter tarmog'iga ruxsatsiz kirish, balki binolarga ruxsatsiz kirishni ham qo'shish maqbul.

*3. **Vakolatning ortishi.*** Bu punktni oldingisi bilan birlashtirilish mumkin, lekin ularning ajratilishi maqsadga muvvofiqdir. Ruxsatsiz kirish deganda tashkilotning resurslari yoki binolariga kirish huquqiga ega bo'lmagan shaxslarning kirishi tushuniladi. Bu tizimga kirish uchun huquqqa ega bo'lmagan tashqi tajovuzkordir. Vakolatning ortishi - tashkilot xodimlarining har qanday manbalariga va binolariga ruxsatsiz kirish huquqidir.

*4. **Virusli hujum.*** Bunday holda, quyidagilarni tushunish kerak: xodimning kompyuterida bitta virusli hujum atroflicha ko'rib chiqishga olib kelmasligi kerak, chunki bu inson omiliga bog'liq bo'lishi mumkin. Agar tashkilotning kompyuterlari sezilarli darajada zararlangan bo'lsa, unda to'liq inshootni xavfsizlik bilan bog'liq zararlanish manbalari, sabablari va h.k.lar uchun kerakli izlanishlar bilan ta'minlanishi kerak.

*5. **Qaydlar ro'yxatining kompрometatsiyasi.*** Ushbu punkt 3-punkt bilan umumiy fikrga ega. Agar foydalalnuvchi insident vaqtida jismonan va aslan o'zining qayd ro'yxatlarini qo'llay olmasa, insident 3-punktdan 5-punktga o'tadi.

Axborot xavfsizligi insidentlarini tasniflashning asosiy maqsadi insidentga javob reaksiyasi jarayonini ko'rsatishda tizimlilik darajasini oshirish va subektivlikni kamaytirishdan iborat. Ushbu jarayonlar insidentga keyinchalik javob reaksiyasini bildirish uchun insident atributlarini aniqlash va qayd etish yo'li bilan hamda axborot

xavfsizligi insidentlari menedjmentining tizimini tahlil qilish orqali amalga oshiriladi. Axborot xavfsizligi insidentlarini quyidagi funksiyalar bo'yicha tasniflash tavsiya etiladi:

- insidentning qayta yuzaga kelishi ehtimoli bo'yicha;
- insidentlarga sabab bo'lgan tahdid manbalari turlari bo'yicha;
- insidentning sabablari bo'yicha (tasodifiy, qasddan, noto'g'ri);
- insidentni amalga oshirishda jalb qilingan (ta'sir ostiga tushgan) axborot infratuzilma obektlari turlari bo'yicha;
- insident sodir bo'lgan axborot infratuzilmasi darajasiga ko'ra;
- axborot xavfsizligining buzilgan xususiyatlariga (maxfiylik, yaxlitlik, mavjudligi) ko'ra;
- insidentning turi bo'yicha (sodir bo'lgan insident, amalga oshirish uchun urinish, hodisa sodir bo'lishiga shubha-gumon);
- insidentning doirasi va harakati bo'yicha;
- insidentni aniqlash murakkabligi bo'yicha;
- insidentni yopishning murakkabligi bo'yicha.

4.3. Insidentni tadqiq qilish elementlari

Insidentni tadqiq qilish uning yuzaga kelishi uchun mas'ul shaxslarni aniqlash, hodisaning dalillari va izlarini to'plash, tegishli intizomiy harakatlarini ta'riflashni o'z ichiga oladi. Katta shirkatlarda, odatda, axborot xavfsizligi insidentlarini tekshirish bo'yicha komissiya ajratadi (uning tarkibiga insidentlarga javob beruvchi xodim ham mavjud). Insidentlarni tergov qilish bo'yicha ko'rsatma quyidagilarni tasvirlashi kerak: hodisani tekshirish bo'yicha harakatlar (shu jumladan, uning yuzaga kelishi uchun mas'ul shaxslarni aniqlash), dalillarni yig'ish va saqlash qoidalari (ayniqsa, sud tizimida dalillarni qo'llash zarur bo'lishi mumkin) va intizomiy harakatlar qoidalari.

Kompyuter insidentlarini tadqiq qilishning 5 ta elementini ko'rib chiqamiz.

1- element. Nima buzildi?

Quyidagilarni aniqlash juda muhim:

- *insident natijasida qanday tizim jarohatlangan;*
- *qaysi servis buzildi;*
- *qaysi ma'lumotlarga tajovuz qilingan.*

Bu maqsadda, tezkor javob berish uchun oldindan tayyorlangan operativ javob berish uchun utilitlar paketidan foydalanish mumkin. Bu

insident natijasida nima buzilganligini aniqlashga yordam beradi. Ushbu paketga qaysi vositalar kiritiladi va ulardan qanday foydalaniladi.

Birinchidan, qisqa vaqt ichida *yo'q bo'lib ketishi* mumkin bo'lgan ma'lumotlarni aniqlash va to'plash zarur, bu vaqtinchalik fayllar, cookies -fayllar bo'lishi mumkin, lekin faqat ular emas.

Ikkinchidan, normal holatdan chetga chiqishlarning mavjudligini aniqlash uchun *tarmoq ulanishlarini* va tizim faoliyatini tahlil qilishni o'rganish kerak.

Uchinchidan, *jarayonlarni* tahlil qilishni o'rganish kerak, kod jarayonlarda amalga oshiriladi, jarayonlar olib boriladigan fayllar va kutubxonalarda joylashgan kodni bajarishi sababli bu yerda ushbu fayllarning yaxlitligiga e'tibor beriladi.

To'rtinchidan, jarayonlar parametr do'konidan, *reyestrdan foydalanadi,* uning tahlillari qo'shimcha ma'lumotni ochib beradi, bunda turli ro'yxatga olish brauzerlari yordam beradi.

Beshinchidan, barcha jarayonlar *xotirada amalga oshiriladi,* shuning uchun xotira tahlili ham tergov uchun muhimdir.

Muammo shundaki, xotira katta, zararli ma'lumotlar esa kichik va osongina o'n oltinchi dampda yo'qolib qoladi.

Audit tizimi va tarmoq trafigini *monitoring qilish tizimi* ma'lumotlarning yaxlitligini buzishganini sezishga qodir.

2-element. Nima vositasida buzildi?

Quyidagilarni aniqlash juda muhim:

- *konfiguratsiyada xato mavjudmi;*
- *ilovada xato mavjudmi;*
- *tizimda xato yuz berganmi;*
- *protokolda xato yuz berganmi.*

Har bir mavzu uchun jarayonlar, reyestr kalitlari, fayllar, turli damplar va jurnallar haqida ma'lumot qanday yordam berishi mumkinligini batafsil o'rganish uchun modul ajratamiz.

Bu yerda bir muhim narsani o'rganish kerak: insidentlar, jurnal yozuvlari va tizim konfiguratsiyasining bir-biriga mutannosibligi. Buning uchun, har bir servisning o'z jurnallariga bo'lishi, u mahalliy sifatida ham, masofaviy serverda ham saqlanishi hamda turli platformalar turli xil jurnal formatlarini ishlatishi mumkinligini tushunib olish kerak.

3-element. Kim buzgan?

Quyidagilarni aniqlash juda muhim:

- *buzib kirish qaysi tizim orqali sodir bo'lgan;*
- *hujumning yakuniy maqsadi nima edi;*

– *qaysi kompyuterdan hujum boshlangan.*

Turli jurnallardan axborotni xavfsizlik insidentidan oldingi hodisalar bilan bog'lash qobiliyati bu yerda ham asqotadi. Ammo, bu bosqichda avvalgi bosqichlarda to'plangan ma'lumotlardan kelib chiqib tajovuzkor identifikatorlarini aniqlab olish kerak. U IP bo'lishi shart emas, u elektron pochta manzili, ilovadagi hisob, media fayl bo'lishi mumkin.

4-element. Gumondor kompyuterida.

Quyidagilarni aniqlash juda muhim:

– *qanday dastur ishlatilgan;*
– *qanday fayllar ishlatilgan;*
– *hujum qaysi ketma-ketlikda sodir bo'lgan.*

Xarakat, gumondorning kompyuteri yoqilgan yoki yoqilmaganligiga bog'liq. Agar o'chirilgan bo'lsa, metodologiyaga ko'ra, endi yoqilmaydi, lekin diskning nusxasi olinadi va keyinchalik AccessData FTK va EnCase kabi vositalarni ishlatib, dalillar topib, hisobot tuziladi. Dalillar kompyuterdan emas, balki printer, kseronusxa apparati, mobil qurilma kabi boshqa vositalardan topilishi mumkin.

5-element. Oldingi elementlarni asoslash.

Quyidagilarni aniqlash juda muhim:

– *nima dalil bo'lishi mumkin?*
– *dalillarni qanday to'plash mumkin;*
– *dalillarni qanday tahlil qilish kerak;*
– *qanday qilib tadqiq qilish hisobotini tayyorlash kerak.*

Damplar, loglar, fayllar - kompyuter terminlari. Ularni rasmiylashtirilgan tadqiq jarayoniga qo'shilish uchun ular dalillar sifatida hujjatlashtirilishi va dalillarning huquqiy ahamiyatini saqlab turadigan tartiblarga muvofiq qayta ishlanishi kerak.

Tadqiqning mohiyati quyidagilardan iborat: tashkilot mutaxassislari hodisani aniqlaydilar yoki o'z-o'zidan insidentga zudlik bilan javob qaytaradilar, ma'lumotlarni tahlil qilib, tahlil natijalarini ma'muriyatga topshirishadi yoki ish yuritishni huquqni muhofaza qilish organlariga topshirilgunga qadar tadqiq qilishni texnik va huquqiy jihatdan qo'llab-quvvatlashni ta'minlaydigan kompyuter insidentlarini tekshirish uchun tashqi ishchilarni yollashadi. Tashkilot hodisalarni o'rganish metodologiyasini qo'llash uchun hodisalarni qonuniy jihatdan tegishli tekshiruvlar o'tkazish niyatida bo'lmasa ham, korporativ axborot tizimining umumiy xavfsizligini oshiradi.

Asosiy xulosalar

Insidentlar, virus infeksiyalarini tadqiq qilishning asosiy maqsadi hujumning oqibatlarini, uning kelib chiqish sabablari va usullarini aniqlashdan iborat. Hujumning sabablari va usullarini aniqlash orqali keyingi hujumlar va infeksiyalarning oldini olish uchun chora-tadbir ko'rish mumkin.

Axborot xavfsizligi insidentlarini tekshirish jarayoni quyidagi bosqichlardan iborat: baholash, yig'ish, tahlil qilish va hisobot.

Insidentlarning tergov bosqichida asosiy rolni: insident jurnallarini saqlash, foydalanuvchi vakolatlarini aniq ajratish, amalga oshgan xatti-harakatlar uchun mas'ul - bu hodisada ishtirok etgan shaxslarning dalillari va amalga oshirilgan harakatlar muhim ahamiyatga ega.

Insident haqida asosiy axborot manbalari: Helpdesk, foydalanuvchidan bevosita xabar, axborot xavfsizligi xodimlari aniqlagan insidentlar, jurnallar va ogohlantirish tizimlari.

Insidentlarni boshqarishda asosiy qiyinchiliklar quyidagi holatlardan kelib chiqadi: hodisani aniqlash va qayd qilish, hodisaning sabablari va oqibatlarini bartaraf etish, hodisani tekshirish, tuzatuvchi va profilaktik harakatlar amalga oshirilishi. Insidentni tadqiq qilish, uning yuzaga kelishi uchun mas'ul shaxslarni aniqlash, hodisaning dalillari va dalillarini to'plash, tegishli intizomiy harakatlarning ta'rifini o'z ichiga oladi. Hodisa va hozirgi vaziyat o'xshashliklarni topish zarur bo'lgan narsalar kabi ko'rinadi va bu holat uchun mavjud bo'lgan faktlarni uzatish orqali ushbu insidentga doir bir nechta xulosa chiqarish mumkin.

Nazorat uchun savollar

1. "Insident" tushunchasi mohiyatini oching.
2. Axborot xavfsizligi insidentlarini tekshirish jarayoni.
3. Insident sodir bo'lganligi haqida asosiy ma'lumot manbalarini tushuntiring.
4. Nimalar insidentlar boshqarishda katta qiyinchiliklarga sabab bo'ladi?
5. Insidentni tekshirishning asosiy bosqichlarini tushuntiring.
6. Xavfsizlik insidentlarining toifalari qanday?
7. Kompyuter insidentlarini tekshirish elementlarining ro'yxatini keltiring.
8. Axborot xavfsizligi insidentlarini hodisa tahlili uchun asos nima?
9. Hodisa tahlil qilish algoritmi modelini tushuntiring.

5. AXBOROT XAVFSIZLIGI INSIDENTLARINING TERGOVI

5.1. Korxonada axborot xavfsizligi insidentlarini tergov qilish

Hozirgi kunda kompyuter texnologiyalarining tarqalishi odatiy holga aylanib, bugun biror-bir korxona yoki tashkilot faoliyatini kompyuter vositalarisiz tasavvur qilish qiyin. Ular yangi va yangi faoliyat doiralariga joriy qilinmoqda, ular zimmasiga yanada ahamiyati, jiddiyroq bo'lgan masalalar yuklatilmoqda.

Axborot xavfsizligi insidenti tergovi tushunchasi va sodir etganlik uchun javobgarliklar

Ammo dunyo miqyosida tobora kengayib borayotgan ilmiy-texnikaviy rivojlanish jarayonlari bilan bir qatorda, ilgari mavjud bo'lmagan jinoyatlarning turlari, shakllari va ko'rinishlari yuzaga kelmoqda, ya'ni axborot texnologiyalari sohasi bilan bog'liq jinoyatlar vujudga kelib, ularning soni ham, turi ham ortib bormoqda. Ushbu holat, o'z navbatida, qonun chiqaruvchidan kechiktirib bo'lmaydigan choralar ko'rishni talab qildi. Binobarin, bu borada mamlakatimizda ko'pgina ishlar bajarildi va axborot tizimlari sohasidagi jinoyatchilikning oldini olish va unga qarshi kurash faoliyatini tartibga soluvchi bir qator normativ-huquqiy hujjatlar qabul qilindi.

O'zbekiston Respublikasining «Axborot olish kafolatlari va erkinligi to'g'risida»gi, «Axborot erkinligi prinsiplari va kafolatlari to'g'risida»gi, «Axborotlashtirish to'g'risida»gi qonunlari, Vazirlar Mahkamasining «Elektron raqamli imzodan foydalanish sohasida normativ-huquqiy bazani takomillashtirish to'g'risida»gi qarori 5 va boshqalar shular jumlasidandir.

Shunday qilib, axborot texnologiyalari sohasidagi munosabatlar jinoiy-huquqiy himoyaga ega bo'lib, buning oqibatida yopiq (konfidensial) axborotlar jinoyatning yangi obyekti sifatida shakllandi. Ushbu jinoyatlarni o'ziga xosligini inobatga olgan holda tergov qilish metodikasini ishlab chiqish – bugungi kunda dolzarb muammolardan biri bo'lib turibdi.

Jinoyat prosessida ko'zdan kechirish tergov harakati eng muhim va jinoyat bo'yicha eng ko'p axborot to'play olish imkonini beradigan tergov harakatlaridan biri hisoblanadi.

Bundan tashqari, tergov harakatiga axborot texnologiyalari sohasidagi mutaxassisni jalb qilish imkoni bo'lmaganida insident joyida tergovchining alohida e'tibor berishi lozim bo'lgan holatlar va tergov-

tezkor guruhi rahbari sifatida amalga oshirishi lozim bo'lgan vazifalari yoritilgan.

Insident sodir bo'lgan joyni ko'zdan kechirish va dallilarini to'plash hamda saqlash.

Axborot texnologiyalari sohasidagi jinoyatlar bo'yicha o'tkaziladigan insident sodir bo'lgan joyni ko'zdan kechirish tergov harakati eng muhim va jinoyat bo'yicha eng ko'p axborot to'plash imkonini beradigan tergov harakatlaridan biri hisoblanadi. Ushbu tergov harakati bir qator muhim sharoitlarni, jumladan:

- o'rganilayotgan insidentni asosiy xususiyati, unda jinoyat tarkibi mavjudligi;
- jinoyatning sodir etilgan joyi va vaqti; jinoyatda ishtirok etganlarning harakatlari nimadan iborat bo'lganligi;
- maqsadlar va motivlar; insident sodir bo'lgan joyda qanday predmetlar yoki narsalar qoldirib ketilganligi;
- jinoyat sodir etgan shaxslar qanday qilib insident sodir bo'lgan joyga kirib chiqqanligi, u yerda qancha vaqt bo'lganligi;
- tajovuz predmetiga yetib borish va u bilan noqonuniy harakatlar sodir etish uchun qanday texnika vositalari va hujjatlardan foydalanilganligi;
- real voqealarni yashirish uchun qanday harakatlar amalga oshirilganligi;
- salbiy oqibatlar va ularning izlari yuzaga kelishini qayerdan izlash lozimligi;
- salbiy natijalarni yuzaga kelishiga nima sabab bo'lganligi va boshqalarni aniqlash imkonini beradi.

Shuni ta'kidlash joizki, «insident sodir bo'lgan joy» va «jinoyat joyi» bir xil bo'lmasligi mumkin. Jinoiy harakat bir joyda, masofadan kompyuter tarmoqlari orqali sodir qilingan bo'lishi mumkin, uning oqibatlari esa boshqa joyda yuzaga keladi.

Aniq tergov vaziyatga qarab tergov-tezkor guruhi tarkibiga quyidagi xodimlar kiradi:

– axborot sohasidagi jinoyatlarni tergov qilishga ixtisoslashgan tergovchi (tergov-tezkor guruhi rahbari);

– axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurash bo'limi xodimi;

– jinoyat sodir bo'lgan hududga biriktirilgan tezkor xodim;

– ushbu turdagi jinoyatlarning izlarini topish, tadqiq qilish, qayd etish va olish sohasidagi ma'lum bilimga ega bo'lgan kriminalist-mutaxassis;

– tergov harakati jarayonida ko'zdan kechirilishi lozim bo'lgan hisoblash texnika vositasi bo'yicha mutaxassis;

– jinoyat izlari topilganda o'tkazilgan texnologik jarayon haqida yetarli bilimlarga ega bo'lgan mutaxassis;

– jinoyat ta'siriga duch kelgan raqamli axborot (uning raqamli axborot tashuvchisi yoki hisoblash texnika vositasi) uchun moddiy javobgar shaxs;

– arizachi yoki jabrlanuvchi.

Yuqorida ko'rsatilgan tergov-tezkor guruhi a'zolari tergovchiga atrof muhitni o'rganish va qayd etish; dalillarni topish, qayd etish, olish va saqlash; insident sodir bo'lgan joyda kerakli dalillarni dastlabki tadqiq etish; kelgusi tadqiqotlar uchun kerak bo'ladigan obyektlarni ajratib olish; jinoyat sodir bo'lishiga imkon bergan sharoitlarni aniqlash; bayonnomada o'ziga xos bo'lgan izlarni yoritib berish; tergov harakati jarayonida texnik vositalarni ishlatish; reja, chizmalar va sxemalar tuzish; jinoyatchilarni, guvohlarni va jabrlanuvchini qidirishda samarali yo'nalish tanlash va hokazolarda yordam ko'rsatadi.

Mazkur tergov harakati oldindan tayyorlanib, batafsil rejalashtirgan bo'lishi kerak. Dastlab quyidagi ishlarni amalga oshirish maqsadga muvofiq:

– vujudga kelgan tergov vaziyatidan kelib chiqqan holda tergov harakatida ishtirok etuvchi shaxslarni aniqlash;

– har bir tergov-tezkor guruhi a'zosiga maqsadlar va harakatlar ketma-ketligini aniq va ravon belgilab berish;

– tegishli mutaxassislarni jalb qilish va ularga kerak bo'ladigan texnik vositalarni olib kelishlarini uqtirish (tergovchi va ekspert-kriminalistning ixtiyorida bo'lgan texnik vositalardan tashqari);

– tergov harakatini boshlashdan oldin ishtirokchilarga ularning huquq va majburiyatlarini, qo'yilgan maqsadni, shuningdek insident sodir bo'lgan joyda harakatlanishda va maxsus moddalar bilan ishlashda ehtiyot choralarini tushuntirib o'tish;

– xolislarni tanlab olish, yo'riqnoma o'tkazish hamda huquq va majburiyatlarini tushuntirish. Xolislarni tanlashda kompyuter axboroti sohasida yetarli (o'rtacha shaxsiy kompyuter foydalanuvchining bilimidan past bo'lmagan) bilimlarga ega bo'lgan shaxslarni jalb qilish maqsadga muvofiqdir.

Tergov-tezkor guruhi insident sodir bo'lgan joyga yetib kelganidan so'ng tergovchi tomonidan quyidagi ishlar amalga oshirilishi lozim:

1. Insident sodir bo'lgan joyga ishga aloqasi bo'lmagan shaxslarni kirishini va obyektning qo'riqlanishini ta'minlash. Bundan shartli ravishda quyidagilar qo'riqlanishi lozim:

- insident sodir bo'lgan joy hududi;
- jinoyat izlari aniqlangan hisoblash texnika vositasi o'rnatilgan joy;
- texnologik jarayonni boshqaradigan va oxirgi operasiyalar to'g'risida ma'lumotlarni saqlaydigan lokal tarmoq serveri;
- elektr tok manbaini o'chirish nuqtalari (agar texnika vositalari yoqilgan holatda bo'lgan taqdirda).

Ushbu vaziyatda quyidagilar e'tiborga olinishi kerak: hisoblash texnika vositasining klaviaturasida ishlash, uni elektr tok manbaidan o'chirish (yoki yoqish), lokal tarmoq serveri bilan va periferik vositalar bilan aloqani uzish (yoki ulash) – kompyuter axborotining, raqamli axborot tashuvchilarning va qog'ozli hujjatlarning o'zgarishi yoki o'chirilishiga olib kelishi mumkin. Shuning uchun tergov harakati boshlanishida hisoblash texnika vositasi yoki boshqa elektron vosita yoqilgan (o'chirilgan) holatda bo'lsa, u tegishli mutaxassis tomonidan ko'zdan kechirish tamom bo'lgunga qadar o'z holatida qolishi lozim.

2. Yuz bergan voqeaning asl mazmuni, insident sodir bo'lgan joyda mavjud bo'lgan jihozlarning o'zgarishi, har bir shaxsning tergov-tezkor guruhi kelgunga qadar bo'lgan harakatlariga aniqlik kiritish maqsadida jabrlanuvchi (arizachi), moddiy javobgar shaxs va guvohlarni so'roq qilish (insident sodir bo'lgan joyni batafsil ko'zdan kechirish jarayonida aniqlanadigan savollar oydinlashtiriladi);

3. Tergov-tezkor guruhi insident sodir bo'lgan joyga yetib kelganda yuzaga kelgan vaziyatni bayonnomada qayd etish, oriyentirli yoki obzorli foto yoki videoyozuvni amalga oshirish;

4. Insident sodir bo'lgan joyga chiqqan tergov-tezkor guruhi a'zolariga topshiriqlar berish. Xususan:

a)hududiy tezkor vakilga – insident sodir bo'lgan joyni chizmasini tuzish, ushbu chizmada insident sodir bo'lgan joyni ko'zdan kechirish jarayonida aniqlangan barcha izlar o'z aksini topishi lozimligini tushuntirish. Chizma tuzishda hisoblash texnika vositalari bir-biriga va periferik vositalarga ulanganlik holati, kompyuter axborotiga kirish huquqini chegaralovchi qo'riqlash tizimlari, turli xil video kuzatuv qo'riqlash tizimi elementlari va boshqa holatlarni

aniqlashda amaliy yordam ko'rsatish uchun tergov harakatiga jalb qilingan mutaxassis biriktirilishi maqsadga muvofiq. Bundan tashqari, hududiy tezkor vakilga bir qator taktik operasiyalarni o'tkazish to'g'risida topshiriq berish (jinoyatni issiq izidan ochish, ushlangan shaxsning shaxsiy tintuvi, arizachi va guvohlarning so'rovi va hokazo);

b)ekspert-kriminalistga jinoyat izlarini aniqlash bo'yicha vazifalar yuklash;

c)tergov harakati jarayonida ko'zdan kechirilishi lozim bo'lgan hisoblash texnika vositasi bo'yicha mutaxassisga hisoblash texnika vositasining turini, ishlatilish maqsadi, aloqaga chiqish imkoniyatlarini aniqlash, shuningdek ushbu vositaning xotirasida mavjud bo'lgan elektron hujjatlarni va ishga ahamiyatli bo'lgan boshqa kompyuter axborotlarini olishda va bayonnomada qayd etilishida tergovchiga amaliy yordam ko'rsatish kabi vazifalar yuklatiladi.

Axborot sohasidagi jinoyatlar bo'yicha insident sodir bo'lgan joyni ko'zdan kechirishni o'tkazishda "markazdan chetga" (ekssentrik) taktik usulini qo'llash maqsadga muvofiqdir.

Ushbu jarayonda, insident sodir bo'lgan joyning turiga qarab, "markaz" bo'lib jinoyat sodir etilishi mumkin bo'lgan hisoblash texnika vositasi o'rnatilgan joy yoki jinoyat sodir etilishi uchun tayyorlangan vosita ishlab chiqarilgan ish joyi bo'lishi mumkin.

Tergov harakati natijasida tuziladigan insident sodir bo'lgan joyni ko'zdan kechirish bayonnomasida quyidagilarga e'tibor berish lozim:

1. ko'zdan kechirilayotgan obyektning nomlanishi va vazifalariga;

2. ko'zdan kechirilayotgan obyektning hududiy joylashishi, unga kirish yo'llari, uning atrofidagi inshoatlar va ulargacha bo'lgan masofaga;

3. obyektning qo'riqlash tizimi mavjudligiga, mavjud bo'lsa, uning joylashishi va tashqi ko'rinishiga, shuningdek kompyuter axboroti chiqib ketishiga qarshi qaratilgan maxsus himoyalovchi signal vositalariga;

4. jinoyat sodir etilishi mumkin bo'lgan hisoblash texnika vositasining inshoatdagi eshik, oyna, boshqa hisoblash texnika vositalari, video kuzatuv uskunalari (mavjud bo'lgan taqdirda) va boshqalarga nisbatan joylashishi;

5. tergov qiziqish uyg'otgan hisoblash texnika vositasidan tashqari, xonada mavjud boshqa hisoblash texnika vositalari va elektr uskunalarga;

6.jinoyat sodir etilgan hisoblash texnika vositasining aloqa kanallari yoki boshqa hisoblash texnika vositalari bilan ulanadigan texnik vositalari mavjudligiga;

7.jinoyat sodir etilishi mumkin bo'lgan hisoblash texnika vositasining boshqa xonalardagi hisoblash texnika vositalari bilan ulanadigan texnik vositalari mavjudligiga (mavjud bo'lgan taqdirda insident sodir bo'lgan joyni ko'zdan kechirish chegaralari ancha kengayishi mumkin);

8.obyektda, unga kelish-ketish yo'llarida jinoyatchi qoldirgan izlarga;

9.ko'zdan kechirilayotgan hisoblash texnika vositasining hujjatlari mavjudligiga.

Yuqoridagilardan shuni xulosa qilish mumkinki, axborot texnologiyalari sohasidagi jinoyatlar bo'yicha insident sodir bo'lgan joyni ko'zdan kechirish tergov harakatidan tashqari kompleks tezkor-qidiruv va tekshiruv tadbirlari o'tkaziladi, bu esa kechiktirib bo'lmaydigan boshqa tergov harakatlari o'tkazilishiga olib kelishi mumkin, jumladan: tintuv, olib qo'yish, hujjat va predmetlarni ko'zdan kechirish, ushlab turish, so'roq qilish, tanib olish uchun ko'rsatish va boshqalar.

Ichki tergovning maqsadi – sodir bo'lgan insidentga aybdorni topish, yuz bergan insidentning sababini aniqlash, kelajakda bunday xodisalarga duch kelmaslik uchun talab va takliflar ishlab chiqish.

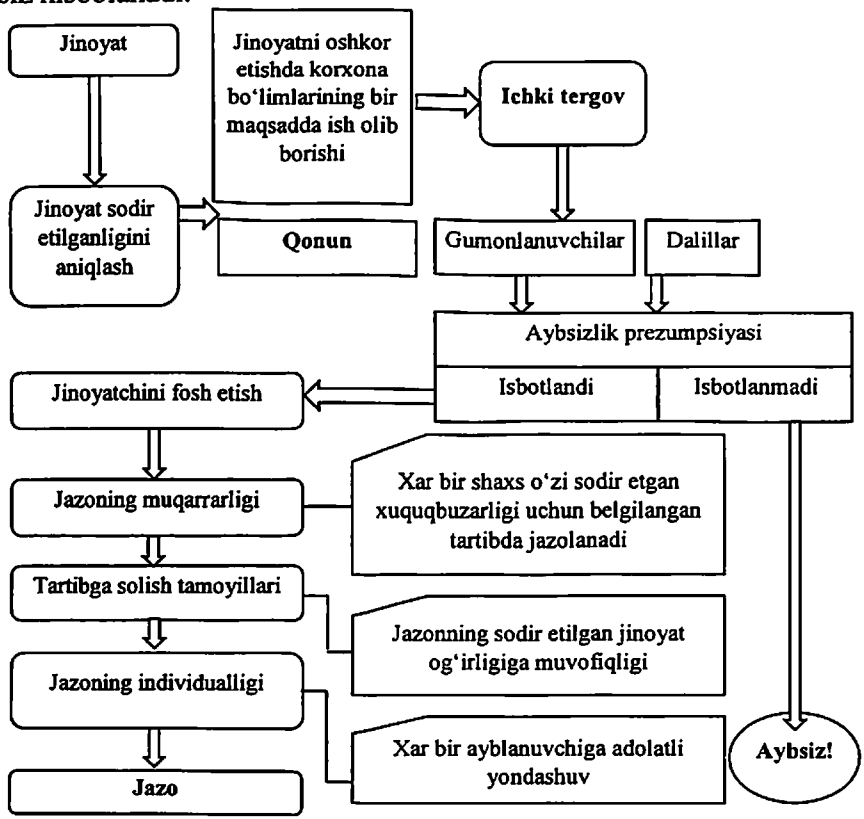
Ichki tergov o'tkazishning asosiy vazifalari: ishchining nima sababdan, qanday vaziyat va sharoitda jinoyat sodir etganligini aniqlash; jinoyatga daxldor aniq bir shaxs yoki shaxslarning aybdorlik darajasini aniqlash; jinoyat sodir etish turlarini, sababini va sharoitini bartaraf etish uchun ogohlantirish-profilaktik turdagi tadbirlar tashkil etish va o'tkazish bo'yicha tavsiyalar ishlab chiqish (5.1-rasm).

Axborot xavfsizligi insidentlarini tergov qilish, aniqlash, taxlil qilish va baxolash. Insidentlarga qarshi chora ko'rishda bu bosqichlarning o'z vaqtida bajarilishi va xaqqoniyligiga qarab, uning muvaffaqqiyatli ishlashini ta'minlab berish.

Jazoning muqarrarligi tamoyilini amalga oshirish - yuridik javobgarlik samaradorligi va uning vazifalarini bajarishda muxim shartlardan biri xisoblanadi.

Ma'suliyat muqarrarligi prinsipi, shahsning rasmiy yoki material holatidan qat'i nazar o'zi sodir etgan huquqbuzarligi uchun belgilangan tartibda jazolanishini anglatadi.

Jazoning muqarrarligi prinsipi ma'suliyat muqarrarligi prinisipi - aybsizlik taxminiga zid bo'lmasligi kerak. Jinoyat sodir etgan har bir ayblanuvchi uning aybdorligi qonunda ko'rsatilgan tartibda isbotlanmagunga va qonuniy kuchga ega hukmda ko'rsatilgunga qadar aybsiz hisoblanadi.



5.1-rasm. Korxonada axborot xavfsizligi insidentlarini tergov qilishni tashkil etish

Ichki tergovni tashkil etish. Asosiy bosqichlar. Korxonada ichki tergov o'tkazishni tashkil etish, ichki xavfsizlik bo'limi zimmasiga yuklatiladi. Ichki tergov o'tkazish uchun korxona rahbari tomonidan komissiya tashkil etiladi. Ayrim xollarda tergov axborot xavfsizligi nazorati markazi mutaxassisi tomonidan o'tkazilishi mumkin. Komissiya a'zolari safiga jinoyatning xususiyatiga qarab, korxonaning xodimlar bo'limi ishchilari va boshqa idoraviy bo'limlaridan ishchi xodimlar kiritiladi. Komissiya ishining bajarilish muddati, to'liqligi va

xolisligi rais tomonidan tashkillashtiriladi, xodimlar tomonidan bajariladi. Tergov o'tkazish muddati odatda korxona rahbari tomonidan ko'rsatiladi. Ichki tergov natijalari tergov yakunlanganidan so'ng xizmat hujjatlari orqali rasmiylashtiriladi. Tergov materiallari ichki xavfsizlik bo'limida bir necha yil davomida saqlanadi, undan keyin arxivga topshiriladi.

5.2. Axborot xavfsizligi insidentlari tergovida guruhlar tuzilmasining modellari

Insidentlarga javob qaytarish guruhi tashkilotning istalgan xodimi uchun ochiq bo'lishi lozim. Insidentni tergov etish qanchalik murakkabligiga qarab unda bir yoki bir nechta ishtirokchilar qatnashishi mumkin. Jamoa rahbari insident guvohlarini tahlil qiladi va guruhda nechta va qanday yo'nalishdagi hodimlar bo'lishi kerakligi haqida qaror qabul qiladi.

Javob qaytarish guruhining tuzilmasini uch xil modeli mavjud:

Markazlashtirilgan model – butun tashkilot doirasida yagona tizim tarzida tashkil qilingan model bo'lib, u uch bo'limdan iborat bo'ladi: call center (telefon qo'ng'iroqlariga javob markazi), texnik yordam markazi (ma'lumotlarni yig'ish va tahlil qilish markazi), tergov qilish guruhi (analitik markaz). Ushbu model uncha katta bo'lmagan tashkilotlar uchun mo'ljallangan.

Taqsimlangan model – markazlashtirilgan model asosida yaratilgan. Ushbu modelning markazlashtirilgan modeldan farqi tashkilot filiallari geografik uzoqlikda joylashganligidadir. Ushbu holatda asosiy ofisning javob qaytarish guruhi axborot xavfsizligi insidentlari haqida muvofiqlashtirish xizmati va ma'lumotlarni saqlash bilan to'ldiriladi.

Korporativ model – sohaga oid markaziy prinsipga asosan amalga oshiriladi. Muvofiqlashtirish bo'limi insidentga javob qaytarish savollari bo'yicha yuridik shaxslardan kerakli ma'lumotlarni oladi, shu bilan birga uning qaramog'idagi tashkilotlarni ham boshqaradi.

Javob qaytarish guruhi hodimlari uch asosiy model ostida yig'ilishi mumkin:

- tashkilot vujudga kelgan insidentni qayta ishlash bo'yicha barcha vazifani o'z zimmasiga oladi va o'z xodimlariga tayanadi;
- jamoa tarkibiga ushbu soha vakillaridan a'zolar qabul qilinadi. Ushbu model o'z resurslariga 24/7 sxemasi ostida ishlaydigan tashkilotlarga to'g'ri keladi. Bunday holatda javob qaytarish va qayta

ishlash masalasini firma o‘z zimmasiga oladi, tergov ishlari bilan esa tashkilot ichidagi guruh shug‘ullanadi;

- insidentga javob qaytarish va uni qayta ishlash ishlari to‘laqonli boshqa tashkilot yoki firmaga yukalanadi. Bu model tashkilotni qo‘lidan qayta ishlash imkoniyati kelmaydigan taqdirdagina qo‘llanilishi mumkin.

Modelni tanlashdagi faktorlar:

1. Axborot tizimi doim 24 soat haftasiga 7 kun mavjudligi.

2. To‘laqonli yoki qisman xodimlar bandligi. Ushbu faktorga agar xodimlar to‘laqonli band bo‘lmasagina ahamiyat berish mumkin. Xodimlar bilan kutilmagan hollarda bog‘lanish yo‘llarini ko‘rib chiqish lozim.

3. Xodimlar mahorati. Axborot xafsizligi insidentlarini qayta ishlash axborot xavfsizligini maxsus dasturiy-apparat vositalarini bilishi talab etadi. Tashkilot ishchi yo‘llashdan oldin ushbu jihatni e’tiborga olishi lozim.

4. Axborot xafsizligi insidentlarini boshqarishni narxi. Tashkilot axborot xafsizligi insidentlarini boshqarish narxini baholashi va o‘zi uchun foydali modelni aniqlab olishi kerak.

5. Tashkiliy tuzilma. Faqat insidentlarni qayta ishlashda korporativ yondashuvdan foydalangan holda axborot xafsizligi insidentlarini tergov etishda erkin harakat qila oladigan jamoalar tuzish mumkin. Bunda eng yaxshi yechim markaziy ofisda muvofiqlashgan markaz tashkil etish bo‘ladi.

Tashqaridan xizmat ko‘rsatish faktorlari:

1. Ko‘rsatilgan xizmat sifatiga javobgarlik. Tashkilot boshqa firma tomonidan bajariladigan ishning sifatini tekshirib boradi. Shuning uchun axborot xafsizligi monitoringini yuritish talab etiladi.

2. Ma’murlik vakolatlarini ajratish. Qurilmani o‘chirib yoqish bo‘yicha daraja, foydalanuvchilar haqidagi ma’lumotlar o‘zgarishi hamda boshqa harakatlar insident yuz berganda kechadigan jarayonlar oldindan kelishib olinishi va hujjatlashtirilishi lozim.

3. Axborotga ruxsatni cheklab qo‘yish. Tashkilot axborot maxfiyligi himoyasini ko‘rib chiqadi. Umumiy holda boshqa firma bizni tashkilot tuzilmasini to‘laqonli o‘rganib chiqishiga imkoniyat yaratib bermaslik kerak (xodimlar haqida malumot, ish yozishmalari, hujjatlarni saqlash katalogi va boshqalar).

4. Tashkilot tuzilmasini bilish. Tashkilot hizmat ko‘rsatuvchi firmaga o‘zi haqida to‘g‘ri tasavvur yaratish uchun harakat qilishi zarur.

Tashkilot insident qanday yuzaga kelgan bo'lishi mumkinligi haqidagi hujjatni yaratadi va har doim uni takomillashtirib borishi lozim.

5. Yuzaga kelgan insident korrelsiyasi. Tashkilot axborot xafsizligi insidenti yuzaga kelganda ushbu vaziyatni korrelasiyalash tizimini ishga tushirishi kerak. Ushbu tizim maxsus bilimni talab qiladi;

6. Insidentlarni qayta ishlash. Tashkilot hizmat ko'rsatish firmasi hodimini insidentni tergov etish jarayonida ishtirok etishi yoki etmasligini aniqlaydi.

7. Insidentlarga mustaqil ravishda javob qaytara olish. Tashkilot axborot xafsizligida yuzaga keladigan insidentlarda mustaqil ravishda javob qaytarishni bilishi kerak. Insident ko'payishi bilan xizmat ko'rsatuvchi firma bilan aloqa uzilib qolishi mumkin. Bunday holatlar uchun tashkilot avariyaviy rejasini ishlab chiqishi kerak.

Tashkilot tuzilmalari bilan aloqa

Moliyaviy tashkilot tanlangan modelidan qat'iy nazar eng kamida ikkita axborot xafsizligiga javob bera oladigan hodimga ega bo'lishi zarur. Ushbu hodimlar kutilmagan insident yuz bergan vaqti muammoni o'zlari bartaraf qilishilari yoki hizmat ko'rsatish tashkilotlari bilan bog'lanishlari kerak bo'ladi. Xodimlar malakasiga qarab yuzaga kelgan insident tez va kam chiqim bilan bartaraf etilishi lozim.

Insidentni qayta ishlash jarayonida tashkilot javob qaytarish guruhiga nisbatan quyidagi siyosatni qo'llashi lozim:

- insidentlarni qayta ishlashni moliyalashtirish tartibi;
- javob qaytarish guruhi xodimlarini boshqa yo'nalishlarda malakasini oshirish;
- normativ va texnik hujjatlarni yozishda javob qaytarish guruhi azolarini ham biriktirish;
- jamoa markazi to'liq birlashgan bo'lishi lozim va hamma o'z vazifasini to'liq bilishi shart;
- ishchilar rotasiyasi amaliyoti doim qo'llab quvatlanishi kerak;
- insidentlar yuzaga kelganda o'zini qanday tutishi kerakligi haqida kurslar tashkil qilish va testlar olib borish;

Insident yuzaga kelgan holatlarda boshqa yo'nalishdagi xodimlarni ham jalb qilish. Masalan yurist, AT muhandisi, hodimlar bilan ishlash bo'limi va boshqalar.

Insidentni qayta ishlash jarayonida tashkilot javob qaytarish guruhining barcha ishtirokchilari umumulashgan holatda ishlashlari zarur.

5.3. Axborot xavfsizligi insidentlarini tergov qilish jarayonidagi qarshiliklar

Axborot xavfsizligi insidentlarini tergov qilish darajasida buzg'unchi tomonidan qarshiliklarga uchrash mumkin. Bunday harakat bir tomonlama yo'naltirilgan yoki umumiy bo'lishi mumkin.

Umumiy qarshi harakatlar. Umumiy qarshi xarakatlar kimgadir yoki nimagadir yo'naltirilmagan bo'lib ko'pchilik hollarda ikki xil vazifani bajaruvchi resurslardan foydalaniladi (misol, fayl tizimi shifrlashini yaratuvchi dasturlar yoki tarmoq trafigini shifrlovchi dasturlar). Ushbu qarshi harakatning asosiy maqsadi ma'lumotlarni shifrlash, yo'q qilish yoki yashirish yo'llari bilan kriminalistik tadqiqotlardan himoya qilishdir.

Yo'naltirilgan qarshi harakat yoki kriminalistik harakatni aldash, ushbu harakatning asosiy yo'nalishlaridan biri hisoblanadi. Ushbu turning asosiy maqsadi: kriminalistik izlanishlardan ma'lumotlarni saqlash, kriminalistik usullar ishonchsizligini ko'rsatishdir.

Ushbu harakatning boshqa turida kriminalistik tekshiruv olib borayotgan tashkilot tarmog'iga ruxsatsiz kirib ma'lumotlarga o'zgartirish kiritishdan iborat hisoblanadi (buning uchun dasturlar va qurilmalarning zaif qismlaridan foydalaniladi). Eng ko'p tarqalgan usullardan biri bu umumiy qarshilik harakatlari hisoblanadi. Maqsadga yo'naltirilgan qarshi harakatlar kam o'rganilgan bo'lim hisoblanadi.

Qarshilik harakatlarining umumiy usullari. Eng ko'p tarqalgan qarshilik harakatlaridan biri bu- ma'lumotlarni himoyalash bu-shifralash, stenografik yashirish, qayta yozish yoki o'chirib tashlash hisoblanadi.

Shu bilan birga hozirgi kunda kriminalistik izlanishlarda mumkin bo'lgan ma'lumotlarni yo'q qilishga qaratilgan usullar ham ko'pdir. Bunday dasturlar operativ xotirada ishlaydi. Bunday usullar va dasturlar ko'p hollarda shaxsiy ma'lumotlarni konfidensial(maxfiy) saqlash uchun yoki so'z erkinligini saqlab qolish uchun ishlatiladi.

Yuqorida sanab o'tilgan usullar qo'llanilishi kiberjinoyatni ochish uchun katta to'siq hisoblanadi, ammo bir qancha kriminalistik usullar mavjudki ular shunday himoyalangan ma'lumotlarni topish va ochish uchun mo'jallangan hisoblanadi.

Insidentlarni tergovga qarshi maqsadga yo'naltirilgan usullar. Maqsadga yo'naltirilgan usullar kriminalistik qiymatga ega bo'lgan ma'lumotlarni aniqlash va ularni yo'q qilishdan iborat hisoblanadi. Kriminalistik tergovni aniqlash esa bir qancha usullardan foydalangan

holda amalga oshirilishi mumkin: tarmoq vositalarini ishlash alomatlarini qidirish maqsadida tarmoq trafigini tahlili, ishlayotgan dasturlar tahlili va h.k.

Bir tomonlama yo'naltirilgan harakatlar. Ma'lumotlarni yo'q qilish, yashirish yoki o'zgartirib qo'yish mantiqiy bombalardan yoki kriminalistik dasturlarga qarshi eksploitlardan foydalanishlar orqali amalga oshiriladi(bunday vositalar dastur xatoliklaridan foydalanishi mumkin).

Yo'naltirilgan qarshilik ko'rsatish asosan kriminalistikaning quyidagi zaif joylariga hujum qilishi mumkin:

1. Usul.
2. Vosita.
3. Harakat.

Usul - kompyuter ma'lumotlarini o'rganib chiqish uchun umumiy usullar. Masalan: kriminalistik operasion tizim yuklanishi, u o'z navbatida nusxalashdan himoyalanmagan tarzda ishga tushiriladi, keyinchalik kerakli fayllardan nusxa olish uchun ham ishlatiladi.

Vosita - dastur yoki qurilma hisoblanib, kriminalistik izlanishlarning ma'lum darajasida foydalaniladi. Misol: Kriminalistik Live CD grml.

Harakat - ma'lum bir darajadagi maqsadga yo'naltirilgan harakatlar ketma ketligidir. Masalan: fayllarni nusxalash uchun dastur ishga tushirilishi (natija: diskda mavjud bo'lgan fayllar nusxalanishi) fayllarni indekslash uchun dasturni ishga tushirish (natija kerakli faylni kalit so'zlar yordamida tezdo topib olish).

Yuqorida keltirilgan zaif nuqtalarga qarshi quyidagi harakatlarni keltirishimiz mumkin:

1. Karshi harakat qurilmada maxsus fayllar yaratish orqali: kriminalistik izlanish aniqlansa darxol faylni almashtirib qo'yish.
2. Dasturiy vositalar yordamida qarshilik ko'rsatish.
3. Kriminalistik izlanish olib borilgani haqida fakt ma'lum bo'lgach kriminalistik ishlayotgan dasturlar turlarini aniqlash.

Apparat (yorliqlar). Ko'pchilik kriminalistik harakatlarga qarshi qo'llash mumkin bo'lgan usullardan biri apparat yorliqlar hisoblanadi. Malasan, kriminalistik izlanishlar olib borilishi aniqlangandan so'ng faylga o'zgartirishlar kiritish yoki yo'q qilish bu apparat ichiga kiritilgan yorliq hisoblanadi. Bunday uslub bilan Live CD yoki dasturiy modullardan qutilish uchun foydalanish mumkin. Boshqa misol esa ma'lumotlarni apparatli yo'q qilish hisoblanadi. Bunda kutilmagan

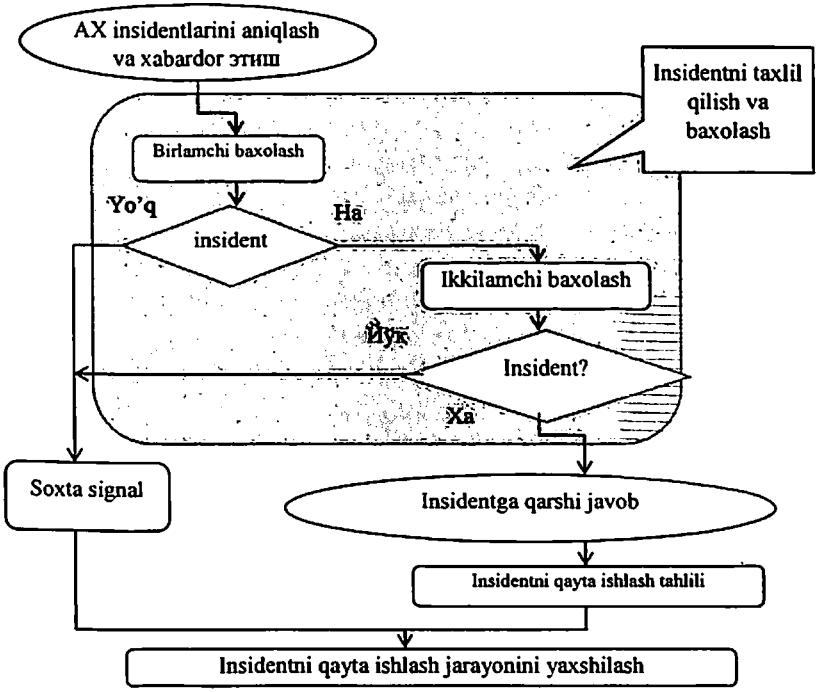
tarzda ma'lumot saqlash qurilmasini ochishga urinishdir. Bunday holatlarda batareya ishga tushadi va uzoq vaqt davomida kuchli tok bilan ta'sir o'tkazadi.

Dasturiy (yorliqlar). Yaqin kunlargacha dasturiy yorliqlar faqatgina ba'zi hollarda o'zini yaxshi ko'rsata olar edi. Masalan Live CD dickka yozishdan himoyalanmagan holda kompyuterni ishga tushirishi mumkin. Xozirgi kunda esa ular ma'lum bir kriminalistik izlanishlarga ham qarshi tura oladigan dasturiy vosita sifatida foydalanilmoqda.

5.4. Korxonada axborot xavfsizligi insidentlarini baholash usullari

Axborot tizimlari sonining o'sishi va axborot texnologiyalarining takomillashgani sari, axborot xavfsizligidagi insidentlarning soni ham ortib bormoqda.

Xalqaro standart ISO 27001:2005 axborot xavfsizligi insidentlarini boshqarish tartibini yaratish zarurligiga alohida e'tibor qaratadi. Chunki, Axborot xavfsizligini samarali boshqarish uchun insidentlarga o'z vaqtida javob qaytarish, ularning sababi va kelib chiqadigan oqibatlarning oldini olish zarur.ISO/IEC 27035 xalqaro standarti va GOST R ISO 18044:2007 milliy standartda axborot xavfsizligi insidentlarini boshqarish jarayonlari keltirilgan. xuquqiy-meyoriy xujjatlar, resurslar, ta'minlash kabi masalalar, xususan AX insidentlari tasniflanishi, AX insidentlarini tartiblashda rollarni taqsimlash ko'rib chiqiladi. Ayrim xollarda korxonada AX insidentlarni aniqlash metodikasi yo'q, ishchilar xar doim xam ishdagi asosiy vazifalarning uzilishlariga aloqadar bo'lmaganligi sababli, qanday xodisalar axborot xavfsizligi insidenti ekanligi haqida bilmaydilar.



5.2-rasm. Axborot xavfsizligi insidentlarini qayta ishlashni boshqarish

Axborot xavfsizligi insidentlarini taxlil qilish va baholash ham, sodir bo'lgan insident haqida ma'lumotning, uning kelib chiqish sababi va oqibatining to'liq emasligi qiyin bo'lishi mumkin. Axborot xavfsizligi insidentlari va insidentlarining aktual bazasini yaratish va ta'minlash extiyoji mavjud. Axborot xavfsizligi insidentlari va insidentlari bazasi axborot xavfsizligi insidentlarini tartiblovchilarning shaxsiy tajribasiga asoslanib yaratilishi mumkin. Odatda korxona, xususan yirik firma, kompaniyalarda sodir etilgan axborot xavfsizligi insidentlar xaqida ma'lumotlar, tizimga qayta xavfning oldini olish maqsadida va korxona obro'siga zarar yetkazmaslik maqsadida nashr etilmaydi (5.2-rasm).

Lekin axborot xavfsizligi analitiklari axborot xavfsizligini ta'minlashda korxona ko'rsatmasidan tashqari, ushbu insidentlar sodir bo'lgan muammolarni o'rganish, masalan, ishlab chiqarish va boshqa tashkilotlarda, axborot texnologiyalarida topilgan zaifliklar va muayyan bir muddatdagi axborot xavfsizligi insidentlari statistikasi xaqida

qisqacha ma'lumot taqdim etishadi. Bunday turdagi ma'lumotlar axborot xavfsizligi insidentlari bazasini aktual holatda saqlab turish uchun bazani doimiy yangilab turishda imkon yaratadi. Axborot xavfsizligi insidentlarini taxlil qilish va baxolash axborot xavfsizligi xodisalarini insident sifatida identifikasiya qilish uchun zarur bo'lgan ma'lumot miqdorining kattaligi sababli, ushbu xodisalarning sababi va manbalarini aniqlash xamda salbiy oqibatlarining tarqalishida qiyinchilik tug'diradi, shuning uchun ushbu jarayonlar rasmiylashtirilgan va avtomatlashtirilgan bo'lishi zarur.

Axborot xavfsizligi insidentlarini uning omillari asosida baxolash.

Dastlabki axborot xavfsizligi insidentsi identifikasiyasini axborot xavfsizligi insidenti sifatida baholash, insidentning muayyan bir turiga ko'rsatuvchi AX xodisalari omillari asosida amalga oshishi mumkin. Axborot xavfsizligi xodisasi omili bu – axborot xavfsizligi ishdan chiqqanligiga ishora beruvchi axborot xavfsizligi insidentsi alomati, hamda xavfsizlik bilan bog'liq kutilmagan insident ro'y berishi. Insident omillari axborot xavfsizligi insidentlari tartiblashtiruvchilar tomonidan tizimni monitoring qilish jarayoni va rejalangan tekshiruvlarda, yoki korxona ishchilari tomonidan asosiy ish vaqtida texnik vositalar orqali aniqlanishi mumkin.

Tizimdagi salbiy insidentlar, masalan ishning sekinlashuvi, dasturiy ta'minotning ishdan chiqishi va x.k. har doim ham axborot xavfsizligi insidenti bo'lmaydi, shu sababli ushbu insidentlar omilining faol ekanligini tasdiqlash maqsadida ikkilamchi baholash o'tkaziladi. Ikkilamchi baholash natijalariga qarab insidentning rost yoki yolg'onligi haqida qaror qabul qilinadi. Axborot xavfsizligi insidentini identifikasiya qilish maqsadida mutaxassisga manbadan aniqlangan axborot xavfsizligi insidentlarining ma'lumotlari asosida axborot xavfsizligi insidentlari omillariga mos belgilangan ro'yxatda beriladi. Axborot xavfsizligi insident omillari ro'yxati sodir bo'lgan insidentlar ma'lumotlari bazasi asosida tuziladi va doimiy yangilanib turadi. So'ngra mutaxassis batafsil ko'rib chiqish maqsadida insidentning turini tanlaydi. Tanlangan insident turiga mos ravishda dastur orqali unga ssenariy quriladi. Ishlab chiqilgan dasturiy vositada aniqlangan omillarga tegishli qo'shimcha ma'lumotlar va faolligini tasdiqlovchi insidentlarni yig'ishga asoslangan ikkilamchi baholash funksiyasi ko'zda tutilgan. Izohda xar bir insidentga omillarni tasdiqlovchi yoki inkor etuvchi va ushbu ma'lumotning manbasiga qanday qo'shimcha

ma'lumot kerakligi xaqida ma'lumotlar keltirilgan. Dastur ikkilamchi baholashda tasdiqlangan omillarga mos ravishda insidentning ssenariysini qayta qurib chiqadi. Bundan tashqari, dasturiy vosita omillari belgilanmagan insidentlarning barcha mumkin bo'lgan ssenariylarini qurish imkonini beradi. Bu funksiya insidentlarni qayta ishlovchi mutaxassisga ko'rib chiqilayotgan axborot xavfsizligi insidenti xaqida qo'shimcha ma'lumotlar to'plash va unga qarshi chora ko'rishda qaror qabul qilish uchun haqqoniyligini oshirishga imkon beradi. Dasturiy vosita potensial insident sodir bo'lish ehtimolini alohida ssenariylari bo'yicha salbiy insidentlar nisbiyligiga va ularni oldini olish bo'yicha ximoya choralariga muvofiq baholashga imkon beradi. Buning uchun dasturda 5 darajali ximoya choralari o'rnatilgan, 0 dan (ximoya choralari mavjud emas) 4 gacha (ximoya choralari insident ssenariylarining salbiy xodisalarini oldini oladi). Har bir darajaga z – ximoya choralarining natijaviy koeffisiyenti mos keladi. Masalan, agar 0.25 ga teng daraja oralig'idagi qadam tanlansa, u xolda 1 darajali ximoya choralari uchun natijaviylik koeffisiyenti 0.75 ga teng bo'ladi, (ya'ni ushbu ximoya choralarini qo'llaganda insident insidentlarining sodir bo'lish extimolligi 0.25 ga kamayadi), 2 darajali himoya choralari uchun natijaviylik koeffisiyenti 0.5 ga teng bo'ladi (ya'ni ushbu ximoya choralarini qo'llaganda insident xodisalarining sodir bo'lish extimolligi 0.5 ga kamayadi) va x.k. Insident ssenariylaridagi salbiy xodisalarning sodir bo'lish ehtimolligini quyidagicha aniqlash mumkin:

$$P_{HC} = h_1 z_i$$

Bu yerda

P_{HC} –insidentlarning sodir bo'lish extimolligi, $i = 1, n$;

n –insident ssenariysida salbiy xodisalarning soni;

h_1 – insidentning qaytarilishi;

z_i – insident ssenariysidagi salbiy insidentlarni oldini olishga qaratilgan ximoya choralarining natijaviylik koeffisiyenti.

Insidentning aloxida ssenariy bo'yicha sodir bo'lish extimolligi P_N quyidagi formula orqali aniqlanadi:

$$P_N = \prod_{i=1}^{n} h_1 z_i$$

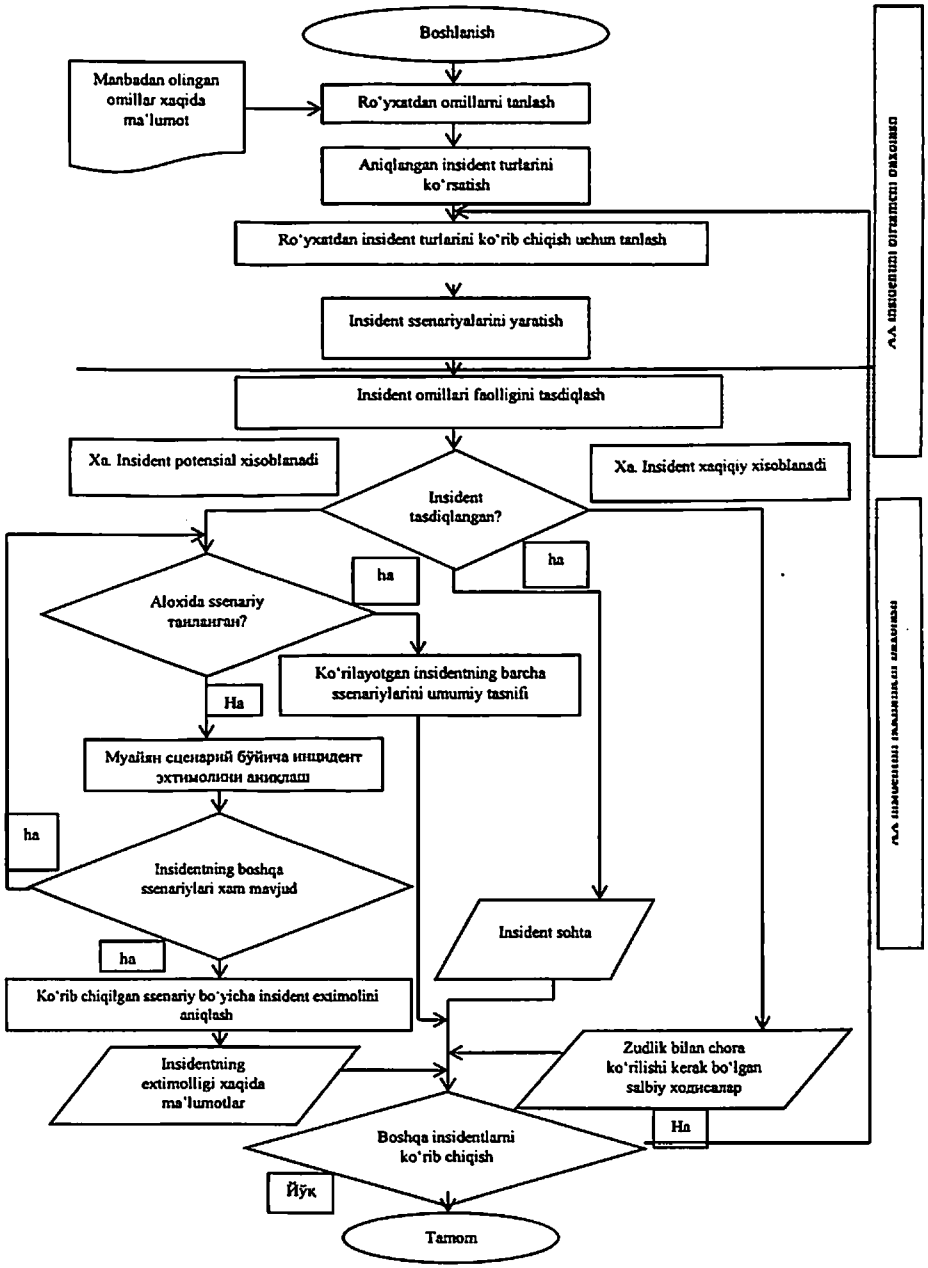
AX insidentining zararli dasturiy ta'minotga tadbiq qilish insidenti misolida alohida ssenariy bo'yicha sodir bo'lish ehtimolligini aniqlash natijasi 5.3-rasmda keltirilgan.

Axborot xavfsizligi insidentlari va insidentlari aktual ma'lumotlar bazasi asosida, tizimda sodir bo'layotgan axborot xavfsizligi insidentlarini baholash imkonini beradi.

Shu orqali vaqtni tejashda va aniqlangan axborot xavfsizligi insidentlarini qayta ishlashda yetarli qaror qabul qilish uchun ma'lumotlarning xaqqoniyligini oshirishga xissa qo'shadi.

Moliyaviy tashkilot tanlangan modelidan qat'iy nazar eng kamida ikkita axborot xafsizligiga javob bera oladigan hodimga ega bo'lishi zarur. Ushbu hodimlar kutilmagan insident yuz bergan vaqti muammoni o'zlari bartaraf qilishilari yoki hizmat ko'rsatish tashkilotlari bilan bog'lanishlari kerak bo'ladi.

Axborot xavfsizligi xodisasi omili bu – axborot xavfsizligi ishdan chiqqanligiga ishora beruvchi axborot xavfsizligi insidentsi alomati, hamda xavfsizlik bilan bog'liq kutilmagan insident ro'y berishi. Insident omillari axborot xavfsizligi insidentlari tartiblashtiruvchilar tomonidan tizimni monitoring qilish jarayoni va rejalangan tekshiruvlarda, yoki korxona ishchilari tomonidan asosiy ish vaqtida texnik vositalar orqali aniqlanishi mumkin.



5.3-rasm. Axborot xavfsizligi insidentlarini baholashning bloksxemasi.

Asosiy xulosalar

Axborot texnologiyalari sohasidagi munosabatlar jinoiy-huquqiy himoyaga ega bo'lib, buning oqibatida yopiq (konfidensial) axborotlar jinoyatning yangi obyekti sifatida shakllandi.

Ichki tergovning maqsadi – sodir bo'lgan insidentga aybdorni topish, yuz bergan insidentning sababini aniqlash, kelajakda bunday xodisalarga duch kelmaslik uchun talab va takliflar ishlab chiqish.

Markazlashtirilgan model – butun tashkilot doirasida yagona tizim tarzida tashkil qilingan model bo'lib, u uch bo'limdan iborat bo'ladi: call center (telefon qo'ng'iroqlariga javob markazi), texnik yordam markazi (ma'lumotlarni yig'ish va tahlil qilish markazi), tergov qilish guruhi (analitik markaz).

Taqsimlangan model – markazlashtirilgan model asosida yaratilgan. Ushbu modelning markazlashtirilgan modeldan farqi tashkilot filiallari geografik uzoqlikda joylashganligidadir. Ushbu holatda asosiy ofisning javob qaytarish guruhi axborot xavfsizligi insidentlari haqida muvofiqlashtirish xizmati va ma'lumotlarni saqlash bilan to'ldiriladi.

Korporativ model – sohaga oid markaziy prinsipga asosan amalga oshiriladi. Muvofiqlashtirish bo'limi insidentga javob qaytarish savollari bo'yicha yuridik shaxslardan kerakli ma'lumotlarni oladi, shu bilan birga uning qaramog'idagi tashkilotlarni ham boshqaradi.

Nazorat uchun savollar

1. Axborot xavfsizligi insidenti tergovi tushunchasi va sodir etganlik uchun qanday javobgarliklarni bilasiz?
2. Ichki tergovning maqsadi nima?
3. Ichki tergovni tashkil etishning asosiy bosqichlari.
4. Markazlashtirilgan model, taqsimlangan model va korporativ modellarning bir biridan farqini tushuntirib bering.
5. Umumiy qarshi harakatlar deganda nima tushunasiz?
6. Qarshilik harakatlarining umumiy usullari.
7. Insidentlarni tergovga qarshi maqsadga yo'naltirilgan usullar.
8. Korxonada axborot xavfsizligi insidentlarini baholash usullari.
9. Axborot xavfsizligi insidentlarini uning omillari asosida baxolashni tushuntiring.

6. AXBOROT XAVFSIZLIGI INSIDENTLARIGA JAVOB QAYTARISH

6.1. Axborot xavfsizligi insidentlariga javob qaytarishni hayot davri prosedurasi

Axborot xavfsizligi insidentlariga tezkor javob qaytarishning asosiy maqsadi insidentning oldini olish (masalan, agar cheklangan ruhsat bilan ma'lumot almashish bloklansa) yoki ehtimoliy zararni tezlik bilan minimallashtirishdir.

Axborot xavfsizligi insidentlariga tezkor javob qaytarish o'z ichiga texnik chora – tadbirlarni, kriminal belgili ma'lumotlar to'liqligini ta'minlash va bu ma'lumotlarning tergov qilish ehtimolligi, hamda insidentdan ko'riluvchi zararni kamaytiruvchi va huquqni himoya qiluvchi organlar uchun hujjatlar tarkibidan va tashkiliy chora – tadbirlardan iborat.

Texnik chora – tadbirlarning asl mohiyati ma'lumot butunligini saqlash, insidentga potensial aloqa, o'chirish yo`llari, aborot saqlovchi mavjud qurilmalarni himoyalash va saqlash. Axborot qurilmasini o'chirish buzg'unchi harakatlar va zararkunanda dasturlarning natijasida kriminal yashirin ma'lumotlarni yo'q qilish ehtimolligini nolga tushuradi, ularni berkitish, belgilash va keraklicha saqlash tergov jarayonlarida keraklicha darajada aniq natijalarni taqdim etadi.

Tashkiliy chora – tadbirlar tashkilot rahbariyatini ogohlantirish, tashkilot bo'limlari axborot xavfsizligi va ularni qiziqtiruvchi insident haqidagi faktlarni o'z ichiga oladi. Tashkiliy chora – tadbirlarni o'tkazish to'g'risidagi hujjatlar jinoiy ishlar bo'yicha tergovda yoki so'roqlarni yo'q qilishda qayta ko'rib chiqish uchun savollarga asoslangan holatda, tashkilot axborot qurilmalarini tergov jarayonlariga ruxsatini begilaydi.

Axborot xavfsizligi insidentlariga javob qaytarilgach insidentning tahlili va tashkilot axborot tizimini qayta tiklash boshlanadi. Tashkilot axborot tizimini tiklash ajratilgan va belgilangan qurulmalarni yangilariga almashtirishni, kerakli DT larni o'rnatishni va axborot xavfsizligi yetarlicha ta'minlash uchun axborot tizimining qaydlarini sozlashni o'z ichiga oladi.

Hujum insidentlari harakatlarining umumiy algoritmlari

Axborot xavfsizligi xizmatining asosiy vazifasi – bu korxona uchun biznesda mavjud usullari, formulalashgan, aniq yo`lni belgilovchi va maxfiylashgan Axborotlarga aloqador zarar yetishi yoki yo'qotilishi

mumkin bo'lgan axborot xavfsizligiga bo'ladigan xavf – xatarlarni oldini olish.

Axborot xavfsizligi sohasida korxona majburiyatlari, barcha umumiy prinsip va huquqlar, korxona uchun rejalashtirilgan mavjud va formal rejalar "Axborot xavfsizligi siyosati" hujjatida keltiriladi. Ushbu hujjatda xavfsizlik hodimlarining axborot xavfsizligiga insident xuruji amalga oshganda qanday harakatlarni amalga oshirishi aniq va qadamma – qadam keltiriladi.

Axborot xavfsizligini buzishdagi odatiy ssenariylar quyi bazaviy harakatlarni amalga oshirishga asoslangan bo'lishi mumkin. Axborot xavfsizligi insidenti jarayonida quyidagilarni amalga oshirish zarur:

1. insidentni identifikatsiyalash va u shu yerda amalga oshirilganiga ishonch hosil qilish.
2. amalga oshayotgan insidentda AT – infrastrukturasini lokallastirish.
3. mavjud insidentga, obektlarga murojaat huquqini cheklash.
4. qayd yozuvlarini insidentlarga javob qaytarish bo'limi rahbari nomiga rasmiylashtirish.
5. konsultatsiya uchun malakali muassislarni jalb qilish.
6. insidentlarni tahlillovchi guruhni yigish va dalillarni to'plash va tizimni tiklash bo'yicha ish rejasini tuzish. Barcha harakatlarni, shu jumladan insidentlarga javob qaytarish usullarini protokollashtirish.
7. dalillarni saqlash va kerakli o'tkazmalarni ta'minlash.
   7.1. Energiyaga bog'liq axborotlarni ishchi tizimlardan uzish.
   7.2. real vaqtda insident haqidagi axborotlarni yig'ish.
   7.3. quvvat tizimidan uzish.
8. uchinchi mustaqil tomonni bazaviy dalil sifatida axborot qurilmalarini belgilash, namunalarni olish va axborotlarni keyingi tahlil va saqlash uchun kiritish.
   8.1. axborot qurilmalaridagi barcha operatsiyalar protokollarini rasmiylashirish.
   8.2. obekt haqidagi ma'lumotlarni yaratish, unga aloqador ma'lumotlar, hatto ularning saqlanish joylarini ham.
   8.3. jarayonlarni foto yoki video kameralarga yozish.
   8.4. chop etilgan obektlarni protokollar bilan birgalikda va ishonchili joyda saqlash zarur toki ular tahlil uchun yoki huquqni muhofaza qiluvchi organlarga yetkazilmaguniga qadar.
9. joriy dalillarni saqlash va yetkazish amalga oshirilgach Axborot tizimining ishchi holatini tiklash lozim.

10. tahlil olib borilayotganda dalillarning o'zgarmasligini ta'minlash. Bunda faqat nusxalar bilan ishlash zarur.

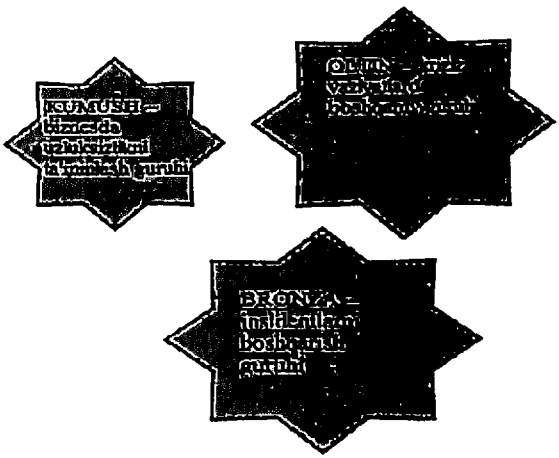
11. izlanishlar olib borilayotganda ishlarni maxsus bo'limlar va tegishli tashkilotlar bilan hamkorlikda olib borilishi kerak (masalan axborot xavfsizligi insidentlarini tahlillash va axborot xavfsizligi ni ta'minlash bo'yicha korxonalar).

12. tahlillar tugagach mavjud hisobotni tayyorlash va kelajakda insidentni yo'q qilish va takrorlanmasilgi ta'minlash uchun tavsiyalar kiritiladi.

13. huquqni muhofaza qilivchi organlar bilan hamkorlikda ishlaganda ularga insident haqida batavsil ma'lumot berish lozim. YA'ni barcha dalillar va analiz natijalari.

Axborot xavfsizligi insidentlarini boshqaruvchanligi

Axborot xavfsizligi insidentlarini boshqarish tizimida ro'yhatga olish, tezkor javob qaytarish va Axborot xavfsizligi insidentlariga ruhsat, hamda insidentlar bilan ishlashning barcha sikli tashkillashtiriladi. Qancha tez va qoniqarli darajada korxona mavjud axborot xavfsizligi insidentlariga javob qaytara olsa bu zarar miqdoriga bog'liq bo'ladi, uning natijasi oldindan ma'lum bo'ladi. Shuning uchun insidentga ruhsatga tayyorgarlik muhim ahamiyatga ega. Tayyorlanish jarayoni rejalashtirish, javobgar shaxsni belgilash, majburiyatlarni taqsimlash insidentlarni boshqarish bo'yicha rejalarni ishlab chiqishni o'z ichiga oladi.



6.1-rasm. Insidentlarni boshqarish strukturasi (PAS 77:2006).

Axborot xavfsizligi insidentlarini boshqarish jarayoni faqatgina ruxsat berish emas, balki ularni tahlil qilish, ruxsat effiktivligini ta'minlash ham muhim. Ishlab chiqilgan rejalarni ishchi muhitning qo'llab – quvvatlashiga testlash va modifikatsilash kerak. Bundan tashqari kuchsiz insidentlarni ham mavjud himoya tizimining darajasini aniqlash va o'zgarishlar kiritish uchun ham tahlil qilish talab etiladi. Agarda tahlil davrida insidentning o'xshash nusxalari aniqlansa, maqbul harakatlar takrorlanadi. Agarda tizim xatoliklari aniqlansa belgilangan rejalar natija bermasa, unda tayyorgarlik bosqichiga o'tiladi.

- Oltin – MCHS, IIV, avariya xizmatlari va organlari tomonidan qo'llab – quvvatlovchi, yuqori menejment tashkilotlari,
- Kumush – xavf – xatarlarni va biznesdagi uzulishlar boshqarish xizmati.
- Bronza – AT va Axborot xavfsizligi markazlari, kadrlarni qo'llab quvvatlash, yuristlar, texnik xavfsizlik va huquqni muhofaza qilish organlari

Muammolar.

Antiviruslar, tarmoqlararo ekranlar, MBBT lar, web-servislar, zaifliklar skanerlari va himoyaning boshqa vositalari axborot xavfsizligi infrastrukturasini to'la ifodalay olmaydi. Himoyaning barcha elementlari alohida sozlanadi va ishlaydi, lekin ular orasida o'zaro aloqador joyi yo'q. Aynan shu himoya kompleksini samarador ishlashini, insidentlarni aniqlashning maksimal tezligini ta'minlaydi.

Axborot xavfsizligi ning markazlashmagan hodisalari monitoring muammolari:

- Axborot xavfsizligi insdentlariga tezkor javob qaytarish;
- Xavf manbaini aniqlay olmaslik va mazkur insidentga javobgarni topish;
- Yeng mushkul tomoni real vaqt rejimida insdent haqida to'liq va ishonchli axborot olish.
- Auditorning axborot xavfsizligi hodisalarini sertifikatlash va tekshiruvlarni oson tahlil qilishni tashkillashtirish.

Yechimlar.

Axborot xavfsizligi sohasida bu muammolorni yechish uchun dastlab Axborot xavfsizligi insidentalarini boshqarish markazini tashkil etish lozim va u quyidagi vazifalarning yechimini topishi lozim:

- Axborot xavfsizligi insidentlarini aniqlash va ularga javob qaytarish vaqtini minimallashtirish;

- Insidentlarni tahlil qilishda axborot xavfsizligi qoidalari va siyosatini bajarilishini nazarot qilish;

- Axborot xavfsizligi holatining markazlashgan monitoringgini tashkil etish;

- Axborot xavfsizligi xavf – xatarlarni boshqarish samaradorligini oshirish va himoyaning kerakli qo'shimcha choralarini ko'rish;

- Korxonaning boshqariluvchanlik va stabillik darajasini oshirish;

- Axborot xavfsizligi hodisalari monitoringgi uchun normative va xalqaro talablarni bajarish;

- Axborot xavfsizligi insidentalarini boshqarish markazini tashkil etishda uning 3 xil asosiy yo`nalishlarini inobatga olish: texnologiya, jarayon va shaxs.

Texnologiyalar.

Texnoligiyalar quyidagi guruhlarga bo'linadi:

- Audit hodisalari;
- Hodisalarni yig'ish, filtrlash, saqlash;
- Hodisalar takrorlanishi va insidentlarni aniqlash;
- Insidentlar tahlili va muammolarni guruhlash;
- Insidentlarni boshqarish bosqichlarida hisobatlarni yuritish;

Kompyuter insidentlarining ekspertizasi.

Bugungi kunda kichik va o'rta biznes korxonalari, banklar va moliya tashkilotlari, davlat boshqaruv organlari va boshqa tashkilotlar kiberjinoyatchilarning qurboni bo'lib qolmoqda va ko'rilgan zarar millionlarni tashkil etmoqda, lekin eng muhimi oddiy aylanib o'tishlar amalga oshirilganida emas, balki, tizim faoliyati va himoyasini baholab, kerakli axborotlarni yig'ib, tashkilot maxfiy ma'lumotlarga ruxsatni berkitib ketishlari, kelajakda bundanda kuchliroq insidentlarni tashkil etishlariga yolg'ochilishidir. Sir emaski, ko'plab korxonalar bunday holatlarga qarshi hech qanday chora ko'rmaydi va faqat zararni qoplash haqida bosh qotiradi, bu esa jinoyatchilarga qo'l keladi.

IBM Security QRadar insidentlar ekspertizasi.

IBM Security QRadar insidentlar ekspertizasi ekspertiza operatsiyalarini o'tqazishda ma'lumotlar paketini olish va boshqasida uzatish uchun ishlatiladi. Bu texnologiya ma'lumotlar qidiruv ishlari boshqaruvi, seanslarni qayta qurish va insidentlardan himoyalanish tahlilini ekspert analizdan o'tkazish imkonini beradi. IBM Security QRadar insidentlar ekspertizasi vositalari dasturiy va apparat ko'rinishida mavjud.

QRadar dan samarali foydalanish uchun dastlab juda ko'p yozuvlar ichidan belgilangan va kelajakda egalik uchun qidiruv va belgilashlarni kiritish lozim, bu bizga cheklangan yozuvlar bilan ishlash imkonini beradi.

Tahlilchilar ishni boshlaganda , ularning materiallari juda ko'p natijalarni qaytarishi mumkin. Agar siz o'zingizga nima kerak ekanligini aniq bilmasangiz, ma'lum bir so'rovni takrorlayverasiz va bu element ustida hech qanday natija bermaydi.

Vizuallashtirish va analizlar natijalar mosligini amaliy yoki avtomatik baholash uchun ishlatilishi mumkin. Bundan tashqari boshqa so'rovlar yordamida ayni muammoga boshqa tarafdan qarash imkonini mavjud

Qachonki siz o'z tahlilingiz bo'yicha kerakli natjaga erishsangiz, uni yanada chuqurroq o'rganish va yakuniy yechimni topish va uni qo'llash uchun ushbu qismni alohida o'rganish imkoniga egasiz. Siz yetarli deb o'ylaganingizdan ko'proq material kiritish lozim.

Tahlil bo'limlarida mavjud relevant natijalar to'plamiga ega bo'lganingizdan so'ng siz o'z izlanishlaringizni aniq yo`nalishga to'g'irlashingiz mumkin. Vizualiatsiaya va tahlil elementlari yordamida har bir qismdagi natijalarni yanada chuqurroq o'rganishingiz mumkin. Ishga aloqador barcha hujjatlarni va yakuniy yechimlarni saqlab qo'yishingiz mumkin. Agar yazuvlar muhim hisoblanmasi ularni o'chirib tashlash mumkin. Izlanishlar jarayonining shu nuqtasida siz turli ma'lumotlar ichidan faqat muhimlarini ajratib olasiz va sizda eng muhin ma'lumotlar to'plami mavjud bo'ladi. Ushbu ma'lumotlar chop etilishi, eksport qilinishi yoki qayta ishlash uchun jo'natilishi mumkin.

Axborot xavfsizligi insidentlarini aniqlashning texnik vositalari va tizimlari.

Himoyaning turli texnik vositalarid hodisalari xavf – xatarlar, ularning buzulishi, mavjud AXBT haqida muhim axborot beradi. Yanada kengroq maqsadlarda, ya'ni tarmoq hujumlarini aniqlash va zararli harakatlarni aniqlashda hujumlarni aniqlash tizimlar (IDS), maxsus ma'lumotlarni tarqalib ketmasligini oldini olish uchun (DLP tizimlari) foydalaniladi, boshqacha qilib aytganda apparat – dasturiy vositalar tarmoq holatini, axborot oqimini, foyadalanuvchilar harakatlarini nazoratda ushlaydi. Axborot xavfsizligi vositalarining zamonaviy tendensiyasi insidentlar haqida va Axborot xavfsizligi tizimi haqida ma'lumotlar olish uchun tor doiradagi daturlardan ko'ra integrallashgan va avtomatlashtirilgan dasturiy apparat vositalar, bir

vaqtda bir nechta vazifalarni bajaruvchi Axborot xavfsizligi ta'minotini talab qiladi.

Asosiy vazifalarni Axborot xavfsizligi insidentlarini aniqlash tizimlari texnik vositalari yordamida hal qilamiz, bular:

- Umumiy hodisalar manbalaridan hodisalarni qayta ishlash orqali saralash va markazlashgan ma'lumotlarni yig'ish.
- Real vaqt rejimida hujumlarni, ZD larni va Axborot xavfsizligi siyosati buzilishlari aniqlash;
- Portlar orqali ma'lumotlar kirishi va chiqishini nazorat qilish;
- Foydalanuvchilar harakatlarining minitoringi;
- Axborot xavfsizligi insidentlarini tahlil qilish uchun barcha dalillarni taqdim etish, ularning bazalarini formallashtirish;

Tahlil olib borish uchun ma'lumotlarni yig'ish uchun turli tizimlar ish jurnallari, hodisalar haqida xabarlar, portlar holatini ko'rish, operatsion tizim jurnallari, ilovalar, protokollar, E-mail xabarlari va biriktirilga fayllarning qaysilari natija uchun zarur va ayni Axborot xavfsizligi insidentni aniqlash uchun fakt ekanligini izlash zarur.

Axborot xavfsizligi insidentlariga javob qaytarishda texnik vositalar va boshqa qo'llab – quvatlashlar.

Axborot xavfsizligi insidentlariga tezkor va samarali javob qaytarish oson, qachonki barcha zarur texnik va boshqa vositalarning qo'llab – quvvatlashlari tayyorlanganda, testlanganda va ayni holatda olinganda. Bu chora – tadbirlar quyudagicha:

- tashkilot aktivlari va biznes funksiyalariga aloqador ma'lumotlarga ruhsat.
- mavjud va amaldagi rejalarga va biznesning uzluksizligini ta'minlovchi hujjatlashtirilgan strategiyalarga ruhsat.
- axborot almashinishdagi hujjatlashtirilgan va barchaga ma'lum jarayonlarga ruhsat.
- axborot xavfsizligi insidentlari va hodisalari electron MB sidan va MB ni to'ldirish va yangilash uchun texnik vositalari, analiz natijalari va javob qaytarish jarayonlari ma'lumotlari foydalanish(tashkilot tomonidan foydalanilgan va talab etilgan yozuvlar).
- rezerv nusxalarni testlash.
- ZD larning nazorati.
- tizim axborotlarining ayni tashuvchilari va DT lar.
- biznes uzluksizligini ta'minlash uchun belgilangan rejaga mos tizim va dasurlar ishonchli va yangilangan versiyalari.

Hujum uyushtirilgan axborot tizimida, xizmatlar va tarmoq noto'g'ri ishlashi mumkin. Shuning uchun tashkilotda foydalanilayotgan texnik qurilmalar ishi (dasturiy yoki dasturiy – apparat vositalar) axborot xavfsizligi insidentlariga javob qaytarishda zarur va lekin faqat tarmoqqa, tizimga va yoki servislarga mo'ljallangan bo'lishiga majbur emas. Axborot xavfsizligi insidentlariga javob qaytarish texnik qurilmalari butunlay avtonom bolishi ham mumkin.

Barcha texnik vositalar puxtalik bilan tanlangan, to'g'ri o'rnatilgan va testlangan (testlashda barcha natijalarda nusxa olinadi) bo'lishi zarur.

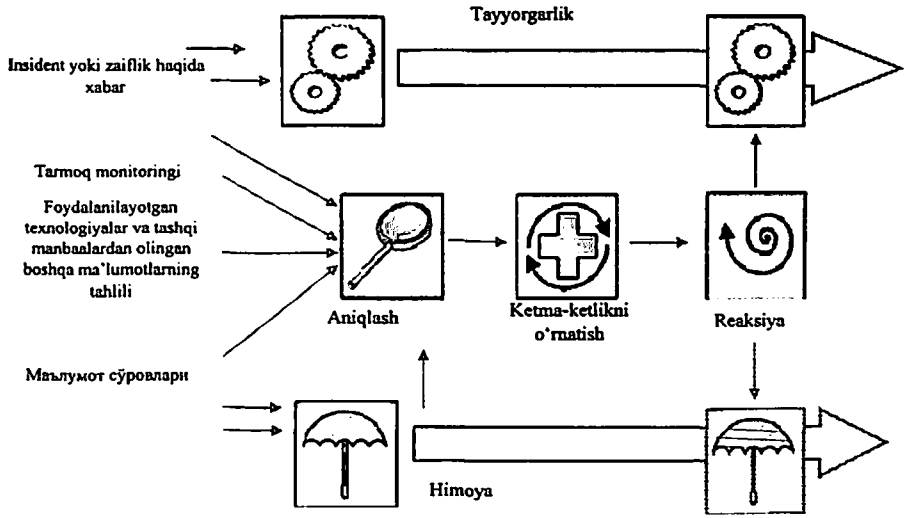
Ta'kidlash joizki, bo'limlarga biriktirilgan texnik vositalar javobgar shaxs kuzatuvisiz avtomatik tarzda axborot xavfsizligi insidentlarini va hujumlarni aniqlashni va qo'shimcha resurslar va qurilmalar ishlatishni o'z ichiga qamrab olmaydi.

Insidentlarga javob qaytarish proseduralari (tartibi)

Biz bilamizki, kompaniyada insident yuzaga kelgan vaqtda jamoalar o'zini qanday tutishi haqida oldindan ishlab chiqilgan proseduralar bo'lishi kerak. Lekin bu qanday proseduralar? Garchi, turli kompaniyalar bu proseduralarni (yoki bosqichlarni) turlicha talqin etsalar ham, lekin aslini olganda ular bir xil vazifani bajaradilar. Insidentlarga javob qaytarish – bu dinamik jarayon hisoblanadi. Uning ayrim bosqichlari parallel holda bajariladi, boshqalari esa ketma-ketlikda, ya'ni keyingi bosqich oldingi bosqich natijalariga bog'liq bo'lgan holda bajariladi. Kompaniya voqea-hodisalarning tegishli hujjatlashtirishlarini ta'minlab beruvchi metodik yondashuvdan foydalanishi juda muhim bo'lib, bu esa insidentlarga javob qaytarish jarayonining keyingi bosqichlarida yoki mabodo ish sudgacha boradigan bo'lsa, va sizdan standart proseduralarga rioya qilganmisiz, ayrim qadamlarni qoldirib ketmagansizmi, deb so'raganlarida muhim ahamiyat kasb etadi. O'tkazilgan tadbirlar va bajarilgan ishlar haqidagi sizning qaydlaringiz sudda maqbul isbot bo'lib xizmat qilishi mumkin.

Insidentlarga javob qaytarish uchun quyidagi proseduralar to'plamini anglab yetish lozim:

- ketma-ketlikning o'rnatilishi;
- lokalizasiya;
- tekshirish;
- analiz;
- kuzatish;
- tiklash.



6.2-rasm. Insidentlarga javob qaytarish proseduralari

Insident oqibatlari tarqalishiga qarshi ta'sir ko'rsatish strategiyasi.

Insident tarqalishiga qarshi ta'sir ko'rsatish prosedurasi – tartibi har bir aniq insident uchun alohida quriladi va uning turiga bog'liq bo'ladi. Qarshi ta'sir ko'rsatish strategiyasining mezonlari shakllantirilgan bo'lishi va javob qaytarish jamoasining barcha ishtirokchilari uchun ruxsat etilgan bo'lishi kerak. Strategiyani aniqlashning mezonlari quyidagi asosiy pozisiyalarni o'z ichiga oladi:

- aktivning potensial shikastlanish (buzilish) ehtimoli yoki o'g'irlanishi;
- insident guvohnomalarini saqlashga bo'lgan talab;
- aktivga kirish mumkinligi;
- qarshi ta'sir ko'rsatishni amalga oshirish uchun zarur bo'lgan vaqt va kerakli resurslar;
- qarshi ta'sir ko'rsatish strategiyasining samaradorligi (muammoning qisman yoki to'liq hal etilishi);
- strategiyaning amal qilish muddati (hafta, oy, chorak va h.).

Bir talay hollarda, yovuz niyatli kimsani o'rganish va insidentga kerakli guvohnomalarni to'plash holatlarida chetga olib qo'yilgan (nazorat qilinadigan) to'xtatish strategiyasi qo'llaniladi, buning mohiyati buzg'unchi hatti-harakatini aniqlash, tahlil qilish, klassifikasiya qilish – tasniflash va nazorat qilish (ta'qib qilish)dan

iborat bo'ladi. Ushbu metodika yuqori darajadagi samaradorlik bilan birga yuqori darajadagi xavf-xatarga uchrash ehtimoliga ham ega, modomiki yovuz niyatli kimsa diskreditasiya (obro'sizlantirish) resursi – usulidan tashkilotning boshqa aktivlariga (faollariga) hujum qilish maqsadida foydalanishi mumkin. Tashkilotda javob qaytarish jamoasining yuqori malakali ekspertlari va axborot xavfsizligi insidentlariga javob qaytarishning ishlab chiqilgan siyosati mavjud bo'lgan sharoitlarda nazorat qilinayotgan to'xtatishning ehtimoli mavjud.

Axborot xavfsizligi insidentlariga javob qaytarishning zaruriy proseduralari

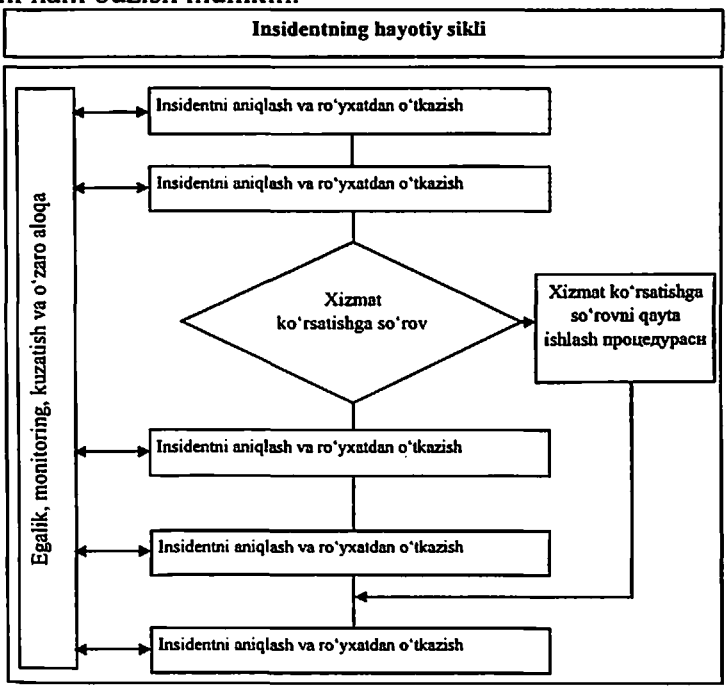
Insidentlarga javob qaytarish prosedurasi bir necha davrdan iborat bo'lib, xodimlarni o'qitish va zarur asboblarni to'plashdan boshlanadi va insidentdan chiqquncha (tekshirishni tugatish va oqibatlarni bartaraf etguncha) davom etadi. Tashkilot tayyorlanish jarayonida korrelyasiya – o'zaro bog'liqlik tizimini to'g'rilab va tashkilot ichi va tashqarisida axborotlar tarqalishi prosedurasini sinchiklab ishlab chiqib, shubhali hodisalarning potensial sonini chegaralashga harakat qiladi. Tayyorlanish jarayonida tashkilot axborot xavsizligi xavf-xatarini baholaydi. Insidentlarning ishlab chiqish jarayonini jiddiy ravishda yengillashtiradigan eng yaxshi amaliyot – bu Axborot Xavfsizligi Menedjment Tizimini (AXMT) joriy etishdir. Insidentni tekshirish ishlari qolgan xavf-xatarlarni baholash prosedurasi va kelgusi ishlar uchun amaliy jihatdan foyda chiqarish bilan yakunlanadi.

Yordamchi jarayonlar strukturasida moliyaviy tashkilotni boshqarish jarayonlarini qo'llab quvvatlanishini ta'minlovchi axborot xavfsizligi insidentlariga javob qaytarish proseduralarini qo'llash uchun rahbariyatning qo'llab-quvvatlashiga muvofiq ravishda axborot xavfsizligini ta'minlash muammosiga yondashuvni qayta ko'rib chiqish talab etiladi.

Axborot xavfsizligini ta'minlash prosedurasini joriy etish mexanizmlari tashkilot jarayonlari tuzilishida yetarli darajada katta hajmli hisoblanadi.

Tashkilotni insidentga javob qaytarish rejasini shakllantirish, u bilan ta'minlash va uni muntazam ravishda testdan o'tkazish muhim ahamiyat kasb etadi. Insidentga javob qaytarishning yaxshi tuzilgan rejasi nafaqat xavfsizlik tizimini buzib kirishdan keladigan zararni, balki jamiyatning salbiy fikr-mulohazalarini ham kamaytiradi.

Xavfsizlik jamoasi nuqtai nazaridan bu buzib kirish qayerdan bajarilganining ahamiyati yo'q (odatda bu narsa ochiq tizim, masalan Internet orqali amalga oshiriladi), eng ahamiyatlisi, u *qachon* sodir bo'lgani. Sizning tizimingiz zaif, unda dadillik yetishmaydi deb bo'lmaydi; shuni tushunib yetish muhimki, yetarli vaqt va resurslarga ega bo'lgan holda hattoki eng qattiq himoyalanadigan tizim yoki tarmoqni ham buzish mumkin.



6.3-rasm. Insidentning hayotiy sikli

Tizimni buzish muqarrarligini anglash ijobiy natijaga ham ega – bu esa xavfsizlik jamoasiga potensial zararni kamaytirish bo'yicha harakatlar yo'nalishini tanlash imkonini beradi. Mavjud tajribaga suyangan holda va ushbu yo'nalishga amal qilgan holda jamoa favquloddagi holatga tez va vahimasiz javob qaytarishi mumkin.

Insidentga javob qaytarish rejasini to'rt bosqichga bo'lish mumkin:

- voqea-hodisa rivojini to'xtatuvchi yoki sekinlashtiruvchi kechiktirib bo'lmaydigan harakatlar;
- insidentni tekshirish;
- tegilmagan, daxlsiz resurslarni tiklash;

- muvofiq kanallar bo'yicha insident haqida ma'lumot berish.

Insidentga reaksiya – javob aniq va tez bo'lishi lozim. Amaliy jihatdan xatolarga yo'l qo'yib bo'lmaydi, shuning uchun bu rejani amaliyotda tekshirib ko'rish va harakatlar bajarilish tezligini o'lchash muhim ahamiyatga ega. Shuningdek, tezlik aniqligi va uni oshirish, o'zlashtirib bo'lmaydigan zararni kamaytirish va tizimning aniq kompрometasiyasi (obro'sizlantirilishi) metodologiyasini ishlab chiqish mumkin.

Insidentga javob qaytarish rejasi o'z ichiga belgilangan talablarni kirgizishi kerak, jumladan:

- kompaniya ekspertlari jamoasi (*Kompyuter insidentlariga javob qaytarish jamoasi*);
- huquqiy jihatdan asoslangan va ma'qullangan strategiya;
- kompaniyaning moliyaviy tomondan qo'llab-quvvatlashi;
- rahbariyatning yuqori darajadagi ko'magi;
- to'g'riligi tekshirilgan va bajariladigan ish-harakatlar rejasi;
- tabiiy resurslar, masalan, ma'lumotlar bazasini takrorlaydigan, kompyuterlarni va zahiradagi nusxalash xizmatini tayyor holatga keltiradigan resurslar.

Insidentga javob qaytarishni amalga oshirish prinsiplari

Tashkilot biznesini uzluksiz boshqarish loyihasini amalga oshirish permanent harakatlanuvchi jarayonlar to'plamini ifodalaydi: tashkilotning tahlili, biznes uzluksizligini boshqarish strategiyasini qaytadan ko'rib chiqish, biznes uzluksizligini boshqarish prosedurasini joriy etish va qaytadan baholash, biznes uzluksizligini boshqarishga ko'maklashish, yaxshilash va audit jarayoni. Biznes uzluksizligini boshqarish prosedurasini joriy etish holatini tahlil qilishning asosiy ma'lumotlar manbalaridan biri bo'lib, axborot xavfsizligi insidentlariga javob qaytarish prosedurasi hisoblanadi.

Jahon amaliyotiga muvofiq ayrim eng yaxshi prinsiplarni shakllantiramiz, qaysiki bu prinsiplarga amal qilgan tashkilot axborot xavfsizligi insidentlariga javob qaytarishning samarali siyosati bilan ta'minlanadi.

Tashkilot rahbariyati tashkilot ichida axborot xavfsizligi insidentlarini tekshirish prosedurasini tadbiq etish uchun zarur shart-sharoitlarni tug'dirishga imkon yaratishi kerak, chunonchi:

- insidentlarga javob qaytarishning rasmiylashtirilgan siyosatini yaratish;
- insidentlarni qayta ishlash proseduralarini ishlab chiqish;

- tekshirish jarayonida ma'lumotlarga murojaat qilishda huquqiy jihatlarni tartibga solish;
- insidentlarga javob qaytarish jamoa tarkibini tasdiqlash;
- insidentlar tergovi bo'yicha jamoaning umumiy mutaxassislari (huquqshunoslar, xodimlar, biznesga ko'maklashuvchi xizmat xodimlari, axborot xavfsizligi va h.) bilan tashkilot ichidagi aloqalarini yaxshi yo'lga qo'yish;
- tergov jamoasining zonalarni belgilash bo'yicha javobgarligi, tekshiruv jamoasini o'qitish va texnik jihatdan jihozlash.

Axborot xavfsizligi insidentlariga javob qaytarishning texnik va boshqa tomondan qo'llab-quvvatlanishi

Qachonki texnik va boshqa ko'maklashuvchi zarur vositalar olingan, tayyorlangan va testdan o'tkazilgan bo'lsa, AX insidentlariga tez va samarali javob qaytarishni amalga oshirish bir muncha oson bo'ladi. Bu chora-tadbirlar quyidagilarni o'z ichiga oladi:

- tashkilot aktivlari detallari – qismlariga (aktivlarning yangilangan ro'yxati mavjudligi afzal) va biznes-vazifalar bilan bog'liq ma'lumotlarga kirishga ruxsat etiladi;
- biznes uzluksizligi ta'minlanishining hujjatlashtirilgan strategiyasi va unga muvofiq rejalarga kirishga ruxsat etiladi;
- ma'lumotlar uzatilishining hujjatlashtirish va bosib chiqarilish jarayonlari;
- AX insidentlari voqea-hodisalari to'g'risidagi ma'lumotlar bazasini tezda to'ldirish va yangilash, javob qaytarish jarayonida ma'lumotlarni tahlil qilish va soddalashtirish uchun ma'lumotlarning elektron bazasi va texnik vositalardan foydalanish (garchi hamma tan olgan bo'lsa ham, ba'zan qo'lda qayd etilgan yozuvlar ham talabga javob beradi va tashkilot tomonidan foydalaniladi);
- AX insidentlari voqea-hodisalari to'g'risidagi ma'lumotlar bazasi uchun biznes uzluksizligini ta'minlanishning adekvat chora-tadbirlari.

AX insidentlariga javob qaytarish jarayonini yengillashtirish va ma'lumotlar bazasi va axborotlar mazmunini tahlil qilishda, ma'lumotlar bazasini tezda to'ldirish va yangilashda foydalaniladigan texnik vositalar quyidagilarga ko'maklashishi kerak:

- AX insidentlari va voqea-hodisalari to'g'risida hisobotlarni tezda olish;
- bu vositalar (masalan, elektron manzil, faks, telefon orqali va h.) uchun mos keladigan avval tanlab olingan xodimlarga (bunga

to‘g‘ri keladigan begona shaxslar) xabar bildirish, ya’ni ishonchli aloqalar ma’lumotlar bazasidan yordam so‘ragan holda (bu baza har doim kirish oson bo‘lishi va o‘z ichiga qog‘ozli hujjatlar va ularning nusxalarini kiritgan bo‘lishi kerak) va axborotlarni uzatish vositasi xavfsiz usulda (zarurat tug‘ilganda) bo‘lishi lozim;

- Internet yoki boshqa vositalar orqali amalga oshirilgan tizimga, servis va (yoki) tarmoqqa hujum qilingan vaqtda elektron aloqani eshitishga yo‘l qo‘ymaslik uchun baholasa bo‘ladigan xavf-xatarlarga muvofiq ehtiyotkorlik choralariga rioya qilish;
- Internet yoki boshqa vositalar orqali amalga oshirilgan tizimga, servis va (yoki) tarmoqqa hujum qilingan vaqtda elektron aloqaga kirishni saqlash uchun baholasa bo‘ladigan xavf-xatarlarga muvofiq ehtiyotkorlik choralariga rioya qilish;
- axborot tizimi, servis va (yoki) tarmoqlardagi va barcha ishlab chiqilgan ma’lumotlarni to‘plash jarayoni;
- o‘zgarishlar mavjudligini belgilashda ko‘maklashish uchun va o‘sha tizim, servis va (yoki) tarmoqning ba’zi qismlari va ma’lumotlar o‘zgarishlarga duch kelsa, agar bu baholasa bo‘ladigan xavf-xatarlarga mos kelsa, yaxlitlikning kriptografik nazoratidan foydalanish;
- arxivlashtirish va to‘plangan ma’lumotlarni soddalashtirish (masalan, ro‘yxatga olish jurnalidagi yozuvlar yoki boshqa ma’lumotnomalar o‘rniga raqamli yozuvlarni qo‘llash yoki CD yoki DVD ROM moslamalarida faqat o‘qish uchun mo‘ljallangan tarqatuvchilarni avtonom rejimda saqlashdan oldin);
- AX insidentlari rivojlanishini namoyish qiluvchi, insident jarayoniga ruxsat etuvchi va axborotlar saqlanishini ta’minlovchi choplamalarga tayyorgarlik (masalan, ro‘yxatga olish jurnallari);
- ma’lumotlar tizimi, servis va (yoki) tarmoqlarning shtatli ish tartibini quyidagilar yordamida tiklash:
- zaxiraga olib qo‘yishning optimal – eng qulay prosedurasi,
- zaxirada turgan aniq va ishonchli nusxalar,
- zaxira nusxalarni testdan o‘tkazish, zararli dasturlarni nazorat qilish,
- tizimdagi va amaliy dasturiy ta’minotdagi boshlang‘ich ma’lumotlarni tarqatuvchilar,
- biznes uzluksizligini ta’minlash rejasiga muvofiq tizim va ilovalar uchun kelishilgan ishonchli va yangilangan tuzatishlar (“patchlar”).

Hujum qilingan axborotlar tizimi, servis va (yoki) tarmoq aniq ishlamasligi mumkin. Shuning uchun, AX insidentlariga javob qaytarish uchun zarur bo'lgan texnik vositalar ishi (dasturiy yoki apparat ta'minoti) tashkilotda foydalaniladigan tizim, servis va (yoki) tarmoqlarga asoslangan bo'lmasligi kerak. Imkon boricha, insidentlariga javob qaytaruvchi texnik vositalar to'liq avtonom – mustaqil bo'lishi lozim.

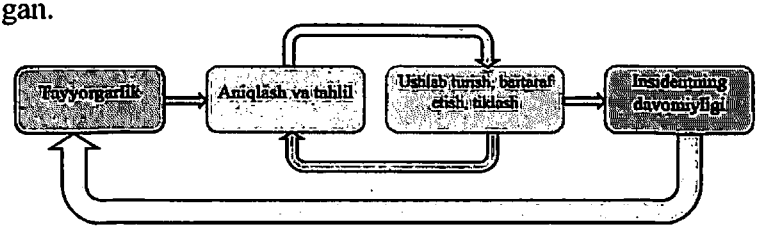
Barcha texnik vositalar sinchkovlik bilan tanlangan, to'g'ri joriy qilingan va muntazam ravishda testdan o'tkazilgan bo'lishi kerak (olingan rezerv nusxalarni testdan o'tkazishni kiritgan holda).

Shuni aytib o'tish kerakki, yo'qorida ta'riflangan texnik vositalar, bevosita AX insidentlarini va ruxsatsiz kirishlarni aniqlash va tegishli shaxslarga avtomatik ravishda xabar berishda texnik vositalarni o'z ichiga olmayi.

Axborot xafsizligi insidentlariga javob qaytarish prosedurasi bir nechta bosqichlardan tarkib topgan. Xodimlarni o'qitishdan boshlab maxsus qurilmalar va insidentlardan chiqib ketishgacha bo'lgan vaqtni o'z ichiga oladi. Tashkilot bunday insidentlarga tayyorgarlik qilish vaqtida har doim kutilmagan insidentlar sonini kamaytirishga intiladi.

Ko'pchilik tashkilotlar bunday hollarda axborot xafsizligi menejmetini qo'llashadi bu esa oz navbatida kutilmagan insidentlarni o'rganishini soddalashtiradi.

Axborot xafsizligini taminlovchi mexanizmlarni ishga tushirish va tashkil qilish ancha katta mehnatni talab qiladi va alohida hizmat korsatish kerak bo'ladi. Insidentlarga javob qaytarish quyidagi darajalarni o'z ichiga oladi: tayyorgarlik, aniqlash va tahlil, ushlab turish/bartaraf qilish/qayta tiklash insidentdan keyingi bosqichlar. Insidentlarga javob qaytarishni hayotiy davri quyidagi 6.4-rasmda keltirilgan.



6.4-rasm. Insidentlarga javob qaytarishni hayotiy davri

1. Tayyorgarlik

Insidentlarga har hil uslublar bilan tayyorgarlik ko'rish, bu faqatgina insidentlarga tayyor turish emas, shu bilan birga ularni oldini olish axborot xafsizligini yaxshilash ham sanaladi.

1.1. Insidentlarni qayta ishlash

Quyida kutilmagan insidentlarni qayta ishlash uchun mavjud bo'lgan qurilmalar va resurslar keltiriladi. Masalan smartfonlar ish harakatni kordinasiyalash uchun yaxshi yechim hisoblanadi. Tashkilot aloqa qilish va ish harakatlarni boshqarish uchun bir qancha yechimlarga ega bo'lishi zarur.

Javob qaytarish guruhi a'zolari bog'lanish uslublari:

- Bog'lanish uchun manzillar guruh doirasida yoki tashqarisida,ya'ni tashkilot ichidan chiqmasdan.
- Insident eslokasiyasi haqida ma'lumot.
- Hisobot mexanizmi.
- Muammolarni boshqarish tizimida insident haqida malumotarni qidirish va boshqalar.
- Shifrlash uchun dasturiy ta'minot, guruh a'zolari o'rtasida aloqa o'rnatish uchun ishlatiladi.
- Insidentni tahlil qilish uchun qurilma va dasturiy taminot:
- Maxsus ishchi stol kriminalistik ishlarni amalga oshirish uchun disklarni nusxalash, fayl jurnallarini olish va boshqa amallarda foydalaniladi.
- Noutbuklar maxsus tashkil qilinadigan yig'ilishlar uchun ishlatiladi.
- Zaxiraviy ishchi stansiyalari va serverlari, tarmoq qurilmalari. Shu bilan birga ularga ekvivalent hisoblanadigan har qanday qurilmalar.
- Xotira qurilmalari.
- Printer, fayl jurnallar va boshqa kerakli bo'lgan dalillarni chiqarish uchun.
- Paket va protokollar analizatori trafikni yig'ish va tahlil qilish uchun.
- Kriminalistik dasturiy ta'minot disklarni tahlil qilish va yig'ish uchun.
- Dalillarni yig'ish uchun boshqa qurilmlar, masalan kamera, diktofon va stiker va bosh.

Insidentni tahlil etish uchun resurslar:

- Portlar ro'yxati, ko'p ishlatiladigan portlar haqida ma'lumot.
- Tashkilotda foydalaniladigan OT dasturlari va protokollari haqida hujjatlar.

- Tarmoq sxemasi.
- Tarmoq va dasturlar to‘g‘ri ishlashi.
- Tekshiruv summalari.

Insidentdan keyingi jarayonni tiklash:

- Avtomatlashtirlgan obrazlarga ruxsat.

2. Aniqlash va analiz

2.1. Xujum yo‘nalishlari. Hujum yo‘nalishlari bu shunday tushunchaki uning ichida hujum qilinishi mumkin bo‘lgan umumiy uslublar keltiriladi va ular quyidagilardir:

- Tashqi xotira qurilmalari.
- Tizim unumdorligini pasayishi.
- Web dasturlar.
- Elektron pochta.
- Ruxsatsiz foydalanish.
- Qurilmalar yo‘qolishi yoki o‘g‘irlanishi.

2.2. Insident alomatlari. Insident alomatlari ikki turga bo‘linadi: bo‘lishi mumkin insidentlar yoki indikatorlar. Bo‘lishi mumkin bo‘lgan insidentlar kelajakda bo‘lish extimoli bor insidentlardir. Indikator esa insident bo‘lib o‘tgani yoki hozirda bo‘layotganini anglatadi.

2.3. Bo‘lishi mumkin bo‘lgan insidentlar va indikatorlar manbalari.

- kutilmagan kirishlarni oldini olish, bartaraf etish;
- xafsizlik jarayonlarini boshqarish;
- zararli dasturlardan himoya qilish va anti spam dasturlari;
- fayllar butunligini tekshiruvchi dastur;
- monitoring hizmatlari.

Jarayonlarni yozish jurnali:

- operasion tizim va dasturlar;
- tarmoq qurilmalari;
- ochiq holda mavjud bo‘lgan yangi zaif tomonlar, hamda eksploytlar.
- Odamlar:
- tashkilot xodimlari.

2.4. Insident tahlili. Quyida insident tahlilini soddalashtirish uchun maslahatlar keltirilgan:

- tizim va tarmoqni indekslash;
- jurnallarni saqlash siyosatini yaratish;
- insidentlar korrelyasiyasini amalga oshirish;
- tizimda bir xil vaqt bo‘lishini kuzatib borish;

- izlanishlar uchun internetda qidiruv tizimlaridan foydalanish;
- qo'shimcha ma'lumotlar olish uchun snifferlardan foydalanish;
- ma'lumotlarni filtrlash;
- ekspertlardan yordam so'rash.

2.5. Insidentni hujjatlashtirish. Insidentni hujjatlashtirishda quyidagilarni hisobga olish zarur hisoblanadi:
- insidentning hozirgi ahvoli;
- insident haqida qisqacha tushuncha;
- insidentga bog'liq indikatorlar;
- ushbu insidentga bog'liq boshqa insidentlar;
- insidentni qayta ishlashda qatnashayotgan hodimlar ish harakati;
- dalillarni yig'ish, ro'yxatdan o'tkazish va saqlashda javobgarlik;
- zararni baholash;
- insidentga bog'liq tomonlarning manzillari;
- tergov jarayonida aniqlangan dalillar ro'yxati;
- insidentni qayta ishlashini sharxlash;
- insident tugagandan keyin qanday harakat qilish kerakligini aniqlash.

2.6. Insidentlarni darajalanishi. Insidentlarni darajalash bu eng muhim bosqich hisoblanadi. Cheklangan imkoniyatlarda eng katta zarar yetishi mumkin bo'lgan qismni aniqlash va bartaraf qilish juda qulay hisoblanadi. Shuning uchun ham insidentlarni guruhlash talab qilinadi.

Insidentning funksional ta'siri:
- mavjud bo'lmagan - xodimlar va tashkilotga hech qanday zarar yetgani yo'q;
- past darajali - tashkilot barcha so'ngi xizmatlarni ko'rsatishi mumkin, ammo pasaygan samara bilan;
- o'rtacha - tashkilot ba'zi foydalanuvchilar uchun xizmat ko'rsata olmay qoladi;
- yuqori - tashkilot juda muhim bo'lgan ba'zi xizmatlarni ko'rsatmaydi.

Insidentga axborot ta'sir o'tkazish:
- ta'sir yo'q - hech qanday ma'lumot o'zgartirilmagan, o'chirilmagan yoki birlashtirilmagan;
- konfidensiallikni buzilishi – tashkilotda konfidensial axborotlarni o'g'irlanganligi;

- butunlik yo'qotilishi - konfidensial ma'lumotlar o'zgartirilsa yoki yo'q qilinsa.

Insidentdan keyingi holat:

- doimiy - kayta tiklash uchun vaqt va resurslar yetarli;
- vaqtinchalik - qayta tiklash uchun vaqt yetarli lekin qo'shimcha resurslar talab qilinadi;
- kengaytirilgan - qayta tiklanish uchun vaqt aniqmas; har tomondan yordam kerak bo'ladi;
- tiklash mumkin emas -insidentdan keyin tiklash mumkin emas, tergov etish kerak.

*2.7. **Insident haqida haqida ogohlantirish.*** Insident tahlil qilib darajaga ajratilganidan keyin, javob qaytarish guruhi javobgar shaxslarga murojat qilishi zarur.

Insidentdan kelib chiqqan holda quyidagi shaxslarga murojat qilish mumkin:

- axborot texnologiyalari boshlig'iga;
- xafsizlik bo'yicha boshlig'iga;
- tashkilot ichidagi insidentlarga javob qaytarish guruhlariga;
- insidentlarga javob qaytarishning tashqi guruhlariga;
- tizim egasiga;
- ishchilar bo'limiga;
- huquqshunosga;
- xonani himoya qiluvchi shaxslarga.

Insident haqida ogohlantirish uchun quyidagi aloqa vositalaridan foydalanish mumkin:

- elektron pochta;
- web sayt;
- telefon qo'ng'roq;
- ovozli pochta;
- qog'ozda yozilgan xat.

3. Ushlab turish, bartaraf etish va tiklash

*3.1. **Ushlab turish strategiyasini tanlash.*** Ushlab turish strategiyasi insident turiga qarab har xil bo'lishi mumkin. Masalan, pochtaga virusli xat kelgan holat bilan DDOS hujum bir-biri bilan katta farq qiladi. Tashkilot har qanday holatlar uchun alohida strategiya ishlab chiqishiga to'gri keladi. Sterategiya esa o'z navbatida quyidagilarni o'z ichiga olishi zarur:

- resurslarni buzish yoki o'g'irlash;
- dalillarni saqlab qolish;

- xizmatlar mavjudligi;
- strategiyani amalga oshirish uchun kerak bo'ladigan vaqt va resurslar;
- strategiya unumdorligi;
- davomiylik.

3.2. Dalillarni yig'ish va qayta ishlash. Har qanday dalil uchun detalli ma'lumotlarni saqlash kerak va ular quyidagilarni o'z ichiga olishi zarur:

- identifikasiyalanadigan ma'lumot (masalan IP-adres , MAC adres va boshqalar);
- insident bilan ishlagan har bir odamning F.I.O., lavozimi va telefon nomeri;
- vaqt;
- saqlash joyi.

3.3. Hujum qiluvchining identifikasiyasi. Hujum qilayotgan shaxsni aniqlash uchun qilinadigan amallar quyida keltirilgan:

- qidiruv tizimlari orqali hujum qilayotgan shaxsni qidirish;
- ichki yoki tashqi ma'lumotlar bazasidan foydalanish;
- hujum qilinishi mumkin bo'lgan kanallar monitoringi.

3.4 Hujumlarni bartaraf etish yoki qayta tiklash. Insidentni aniqlab uni to'xtatishga erishilgandan keyin u yetkazgan zararni qayta tiklashga to'gri keladi. Ba'zi insidentlar uchun qayta tiklash jarayoni qiyin bo'lmaydi.

Qayta tiklash holati ma'lum dastur yoki OT turidan kelib chiqqan holda har xil bo'lishi mumkin.

4. Insidentning davomiyligi

4.1. O'rganilgan darslar. Insidentning ko'rib chiqish qismida quyidagilarni ahamiyatga olish zarur:

- nima boldi va qanday vaqtda?
- xodim yoki javobgar shaxs ishni qay darajada bajara oldi?
- xujjatlashtirish jarayoni amalga oshirildimi? Jarayonlarni analiz qilish shartmi?
- qanday ma'lumot oldin kerak bo'lgan?
- bunday holatlarni oldini olish uchun nimalar qilish zarur?
- tashqi tomonlar bilan aloqani yaxshilasa bo'ladimi?
- qanday harakatlar bunday holatlarni oldini oladi?
- xuddi shunday insidentlarni aniqlash uchun qanday qo'shimcha resurs yoki qurilmalar kerak boladi?

4.2. Insident asosidan yig'ilgan ma'lumotlarni qayta ishlanishi. O'lchash lozim bo'lgan birliklar:

- qayta ishlangan insidentlar;
- har bir insident uchun yo'qotilgan vaqt birligi;
- har bir insidentni qayta ishlash unumdorligi;
- har bir insidentni subyektli baholanishi.

Insidentlarni aniqlashda audit siyosati. Audit mavjud bo'lgan muammolarni ko'rsatib beradi va keyinchalik uni bartaraf etishi mumkin bo'ladi. Eng kam holatda audit quyidagi savollarga javob berishi zarur:

- insidentga javob qaytarish siyosati rejasi va jarayonlari;
- resurs va foydalaniladigan qurollar;
- jamoaning tuzilmasi va modeli;
- insidentni qayta ishlash jarayonida ishtirok etgan shaxslarni qayta o'qitish va malakasini oshirish;
- insident haqida hujjarlar;
- insidentni boshqarish unumdorligini baholash.

Insidentlarga javob qaytarishni hayot davri haqida umumiy ma'lumot olish uchun yuqorida keltirilgan ketma – ketlik bo'yicha ma'lumotlarni umumlashtirish lozim.

6.2. Axborot xavfsizligi insidentlariga javob qaytarish guruxi

Bugungi kunda axborot xavfsizligi insidentlariga javob qaytarish (AXIJQ) dolzarb muammolardan hisoblanadi. Birinchidan, bu mavzu juda ommabop, boshqa tomondan, u mavhumlik muammosi bilan bog'liq, chunki aynan tekshiruv vaqtida tizimning aniq zaif tomonlari, taxdidlarning izlari aniqlanib, AX xodimlarining malakasi, AX tizimining tuzilish sifati tekshiriladi.

Shuni ta'kidlab o'tish joizki, kompaniyada axborot xavfsizligiga bo'lgan hujumlar yashiriladi, sababi hech kim o'z xatolarini tan olishni hohlamaydi va shu bilan raqobatchilarga qo'shimcha asoslar berishni hohlamaydilar. Buning natijasida hujumlarning soni uzluksiz ravishda o'sib boradi, ular to'g'risidagi ma'lumot esa qoida bo'yicha sir saqlanadi va biz OAV da e'lon qilingan kam miqdordagi hujumlar to'grisidagi ma'lumotlargagina ega bo'la olamiz. Boshqa tomondan bunday "aniqlik" kompyuter hujumlarini tavtish etuvchi mutaxassislarni qidirishdagi yoki kompaniyaning hujumlarga javob qaytarish jarayonini tashkil etishdagi qiyinchiliklarni anglatadi. Umuman olganda, aniq sabablarga ko'ra ijrochi o'z mijozlarining bajarilgan ish to'g'risidagi

murojatlarga javob qaytara olmaydi. Shuningdek, bu turdagi ishlarni bajarish ijrochi va buyurtmachi o'rtasidagi ishonchni talab etadi.

Bu turdagi mutaxassisdan nimalar talab etilishini sanab o'tishga harakat qilamiz:

- xavfsizlik prinsiplarini anglash;
- axborot obyektlarining nuqsonlari va zaifliklarini bilish;
- internet qurilmalari haqida tushuncha;
- axborot tizimiga qarshi xavf-xatarlar tahlili bo'yicha ko'nikma;
- tarmoq protokollarini bilish;
- tarmoq ilovalari va servis haqida bilish;
- tarmoq xavfsizligi muammolarini bilish;
- tugun yoki tizim xavfsizligi muammolari haqida tushuncha;
- zararkunanda dasturlar (virus, troyanlar) to'g'risida tushuncha;
- dasturlash malakasiga ega bo'lish.

Axborot xavfsizligi insidentlariga javob qaytarish guruhi (ing. Information Security Incident Response Team (AXIJQG)) bu tashkilotning ishonchli va malakali a'zolari guruhi bo'lib, axborot tizimlariga tegishli belgilangan javobgarlik doirasida axborot xavfsizligining buzilishiga javob qaytarishni bajaradi, koordinatsiyalaydi va jarayonni ushlab turadi.

AXIJQG ni yaratishdan maqsad axborotni yuborish jarayoni va qayta aloqa, boshqarish, kerakli koordinatsiya kabilardan dars olish, bundan tashqari AX Insidentlariga javob qaytarish, baholash uchun tashkilotni mos personal bilan ta'minlashdan iborat. AXIJQG a'zolari AX hujumlariga bog'liq bo'lgan jismoniy va moliyaviy zararni shuningdek, korxonaning nomini tiklashdagi zararni kamaytirishda qatnashishlari mumkin.

AXIJQG tarkibi miqdor, yo'nalish, tashkiliy-huquqiy tuzilma va boshqa kompaniya boshqaruvining xarakteristikalariga bog'liq. Shuningdek, AXIJQG ning minimal tarkibi: AXIJQG bosharuvchisi, registrator-baholovchi, hujumlar registratsiyasi MB administratori, kompyuter sud ekspertizasi mutahhassisi, yurist, tizim masalalari bo'yicha mutaxassis, tarmoq masalalari bo'yicha mutaxassis va axborot xavfsizligi bo'yicha mutaxassis-yekspert.

AXIJQG izolyatsiyalangan guruh bo'lib, personalining asosiy vazifasi hujumlarni tavtish qilish hisoblanmaydi, regitrator-baholovchi va hujumlar registratsiyasi MB administrator bundan mustasno. Axborot

xavfsizligiga hujumning turiga qarab AXIJQG a'zoligiga shartnoma asosida aniq ixtisoslashgan masalalar bo'yicha mutaxassislar olinishi mumkin. Guruh azolari ichki lavozim vazifalaridan kelib chiqqan holda AXIJQG ichida bir qancha funksiyalarni bajarishi mumkin.

Yeslatmalar

Berilgan gruppa tashqi ekspertlar bilan to'ldirilishi mumkin masalan, tan olingan javob qaytarish guruhidan kompyuter hujumlari yoki tezkor javob qaytarish guruhiga.

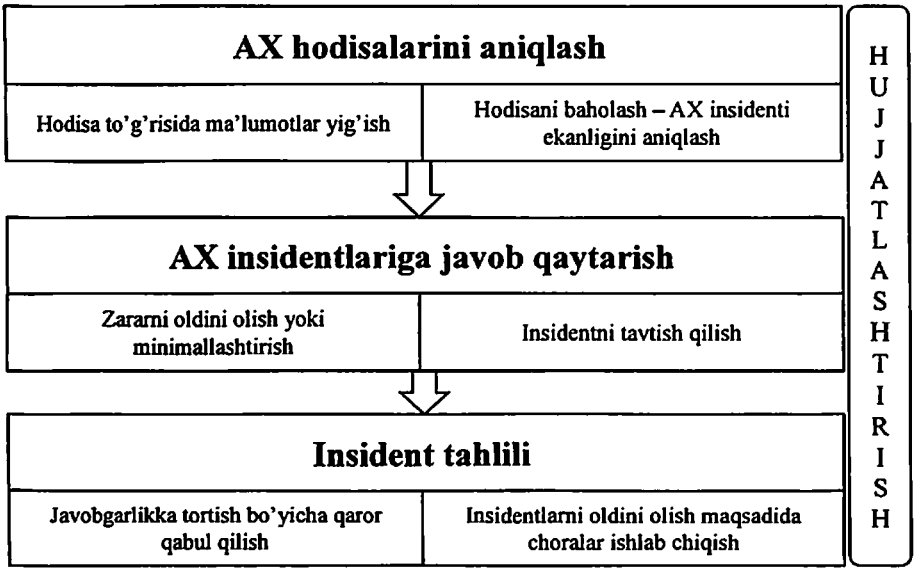
AXIJQG ni yaratishdan maqsad axborotni yuborish jarayoni va qayta aloqa, boshqarish, kerakli koordinatsiya kabilardan dars olish, bundan tashqari AX Insidentlariga javob qaytarish, baholash uchun tashkilotni mos personal bilan ta'minlashdan iborat. AXIJQG a'zolari AX hujumlariga bog'liq bo'lgan jismoniy va moliyaviy zararni shuningdek, korxonaning nomini tiklashdagi zararni kamaytirishda qatnashishlari mumkin.

AXIJQG tarkibi

Ushbu personalning miqdor va tarkibi tashkilot faoliyati maqsadi va masshtabiga mos tushishi lozim.

AXIJQG alohida tuzilgan guruh yoki korxonaning turli bo'limlaridan (masalan, axborot texnologiyalari / telekommunikatsiyalari, buxgalteriya, kadrlar bo'limi va marketing) jalb etilgan xodimlar jamoasi bo'lishi mumkin.

AXIJQG boshqaruv a'zolarini xabardor qilish uchun boshqa biznes jarayonlaridan alohida bo'lgan tizimga ega bo'lishi kerak.



6.5-rasm. AX insidentlariga javob qaytarish guruhining ishlash jarayoni

AXIJQG majburiyatlari

AXIJQG majburiyatlarini 2ta asosiy guruhga ajratish mumkin:

- ***Joriy vaqtdagi harakatlar***, asosiy masala bilan bog'liq – tahdidlarga javob qaytarish;
- ***Profilaktik harakatlat,*** joriy vaqt masshtabida yuzaga kelmaydigan va yordamlashuvchi vazifani bajaradigan harakatlar.

Birinchi guruh kiruvchi hisobotlarni (hujumlar klassifikatsiyasi) baholash va boshqa tashkilotlar(javob qaytarish kordinatsiyasi), guruhlar va internet xizmatlari ta'minotchilari bilan birgalikda qabul qilingan ma'lumotlar ustida ish olib borish, shuningdek, hujumdan so'ng ishni tiklashda(muammolarni hal qilish) lokal foydalanuvchilarga yordam berishni o'z ichiga oladi.

Hujumlar klassifikatsiyasi quyidagilarni o'z ichiga oladi:

- ***hisobotlarni baholash:*** kiruvchi ma'lumot muhimlilik darajasiga qarab tartiblanadi, bunda davom etayotgan hodisalar va aniqlangan tendensiyalarga bog'liq bo'ladi.
- ***tekshiruv:*** hujum va uning masshtabi aniqlanadi

Javob qaytarish kordinatsiyasi o'z ichiga quyidagilarni oladi:

- ***axborotni kategoriyalash:*** hujumga taalluqli bo'lgan ma'lumot (ro'yxatga olish jurnallari, bog'lanish ma'lumotlari va hk) axborotlarni oshkor qilish siyosatiga asoslangan holda kategoriyalanadi.

- ***kordinatsiya:*** axborotlarni oshkor qilish siyosatiga ko'ra boshqalar hujum haqida xabardor etiladilar.

Muammolarni bartaraf etishning vazifalari quyidagilar:

- ***texnik ta'minot;***
- ***muammolarni hal etish:*** hujum va uning paydo bo'lish sabablarini yo'qotish;
- ***qayta tiklash:*** tizimni normal holatga qaytarishda yordam ko'rsatish.

Profilaktik harakatlarga quyidagilar kiradi:

Ma'lumotlar bilan ta'minlash: ma'lum zaif joylar, oldingi muammolar yechish yo'llari yoki konsultatsiya maqsadida havolalar ro'yhatini tashkil etish; xavfsizlik vositalarini taqdim etish (masalan, audit vositalari).

- kadrlarni o'qitish va tayyorlash;
- mahsulotlarni baholash;
- tashkilotning himoyalanganliligini baholash;
- konsultatsiya xizmatlari.

Insidentga mos rollar va funksiyalar

Jarayonlarning realizatsiyasi gorizontal yo'nalishda tashkilotning iyerarxik strukturasi orqali olib boriladi. Bu faqatgina jarayonlarning realizatsiyasiga bog'liq bo'lgan javobgarlik va vakolatlarni aniqlashda yuzaga keladi. Moslashuvchanlikni oshirish maqsadida rolli yondshuvdan foydalanish mumkin (rollarni aniqlash). Katta bo'lmagan tashkilotlarda yoki umumiy harajatlarni kamaytirish maqsadida rollarni birlashtirish mumkin, masalan, o'zgarishlarni boshqarish va konfiguratsiyalarni boshqarish jarayonlari boshqaruvchisi rollarini moslashtirish.

Hujumlarni boshqarish jarayoni boshqaruvchisi.

Ko'plab tashkilotlarda hujumlarni boshqarish boshqaruvchisi rolini Service Desk xizmati menejeri amalga oshiradi. Hujumlarni boshqarish jarayoni boshqaruvchisi javobgarligi sohasiga quyidagilar kiradi:

- jarayonning samarali va ratsional ishi monitoring;
- qo'llab quvvatlash guruhi ishini nazorat qilish;
- jarayonning borishini yanada mukammallashtirish bo'yicha ko'rsatmalar tuzish;
- hujumlarni boshqarish tizimini rivojlantirish va kuzatib boorish.

Qo'llab-quvvatlash guruhi personali.

- qo'llab quvvatlashning 1-qismi ro'yxatga olish, klassifikatsiya, taqqoslash(yechim), qo'llab quvvatlash guruhiga tarqatish, hujumlarni bartaraf etish va yopish.
- qolgan qo'llab quvvatlash guruhlari tavtishda, diagnostikada va hujumlarni bartaraf etishda o'rnatilgan vakolatlar doirasida qatnashadilar.

Service Desk xodimlarining roli va javobgarliklari.

Service Desk – bu mijoz yoki foydalanuvchilar bilan kelishilgan holda taqdim etiladigan servislar yuzasidan javobgar bo'lgan dispetcherlik xizmati emas, barcha talab va takliflarni qabul qilish markazi, joriy servizlarning holatini nazorat qiluvchi va mavjud ishdagi buzilishlarni bartaraf etish uchun naryadlar chiqarish huquqiga ega, shuningdek, buzulishlarni bartaraf etish jarayoni ustida nazoratchi hisoblanadi.

Qo'llab quvvatlash hodimlari javobgarliklarini ajratishda tashkilotning o'lchami va Service Desk va biznes o'rtasidagi xizmat ko'rsatish darajasining asosiy shartlarini hisobga olish lozim. Shuni yodda tutish lozimki, gap mavqelarni emas rollarni tariflash haqida ketyapti. Xizmat masalalarini yechish uchun quyidagi rollarni ajratib olish kerak:

- Qo'llab quvvatlash xizmati menejeri;
- Qo'llab quvvatlash xizmati analitigi.

1. Menejer.

Service Desk menejerining asosiy vazifalari butun xizmat ishining kordinatsiyasi va uning uzliksiz rivojlanishi bilan bog'liq. Uning asosiy vazifalari quyida ko'rsatilgan:

- xizmat analitiklar va kundalik jarayonlarni boshqarish, ishni baholash;
- ish samaradorligining monitoring va uni yanada rivojlantirish bo'yicha tavsiyalar tuzish;
- xodimlarni tayyorlash bo'yicha rejalarini tuzish va amalaga oshirish;
- boshqaruv hisobini ishlab chiqish;
- xizmat doirasida foydalaniladigan jarayonlarni amalga oshirish va yangilarni rivojlantirish;
- xizmat ichida xizmat ko'rsatish madaniyatini shakllantirish.

2. Analitik (muhandis, dispetcher).

Service Desk analitigining roli xizmatning kundalik masalalari va jarayonlarini amalga oshirish bo'yicha javobgarlikdir. Bu rol,

avvalambor, Hujumlarni Boshqarish jarayonini amalga oshirish bilan bog'liq. Hujum hayot siklining boshlang'ich davrida Service Desk analitiklari hujumning aniq registratsiya va kllassifikatsiyasi, boshlang'ich yordam ko'rsatishga javobgardirlar. Boshlang'ich yordam ko'rsatish bosqichida belgilangan vaqtinchalik chegaralar doirasida maksimal miqdordagi hujumlarni hal etishga javobgardirlar. Bu harakatlar to'g'ridan to'g'ri mijozni qoniqtirish bilan bog'liq va yordam ko'rsatish zanjirida hujumning aniqligini belgilaydi. Xizmat analitiklari darhol hal etilmagan hujumlarni hisobga olishga javobgarlar. Bu bilan ularning javobgarliklari tugab qolmaydi, ular xizmat ko'rsatish maqsadlariga mos holda ularni qayta ishlanishini davom etayotganiga kafolat berish maqsadida hujum uchun javobgarlikni saqlab qoladilar. Shuningdek, u mijozga hujumning butun hayot sikli davomida olib borilayotgan ishlar haqida ma'lumot berib boradi.

Hujum hal etilishi bilan analitik mijozning yechimdan ko'ngli to'lganligiga amin bo'lish lozim va shundan keyingina hujumni yopishi mumkin. Bu rol shuningdek, Service Desk ga kelib tushadigan barcha turdagi so'rovlarni boshlang'ich qayta ishlanishini va Service Desk infratuzilmasining knowledge base (bilimlar bazasi) bazasi yoki ko'plab beriladigan savollar ro'yxatini to'ldirib borilishi kabi ichki elementlarini bajarishni o'z ichiga oladi. Bu rol quyidagi harakatlar uchun javobgardir:

Hujumni ro'yxatga olish

- boshlang'ich yordam ko'rsatish jarayonida hal etilmagan hujumlarni hal etish guruhiga yo'naltirish;
- boshlang'ich yordam ko'rsatish va klassifikatsiya;
- barcha ochiq hujumlarni hal etishdagi siljishlar va statusni nazorat qilish;
- so'rovlardagi siljishlar to'g'risida foydalanuvchilarni xabardor qilish;
- lozim bo'lganda hujum eskalatsiyasini amalga oshirish.

Analitikning asosiy sifati doimiy stress holatida ishlashga qodir bo'lish "zarbani qabul qilish"ni bilish, masalalarni yechishda konstruktiv yondashish, shikoyat va ayblovlarga aniq javob berish hisoblanadi.

Bu acceptivlik (qabul qiluvchanlik) deyiladi –qat'iyat butun "negativ" oqimidan foydali axborotni ajratib olish xususiyati, o'sha axborotdan negativni yurakka yaqin olmagan holda foydalanish.

Ikkinchi zarur bo'lgan sifat – bu jamoada ishlay olish qobiliyati. "Yulduzlar" emas, birgalikda ishlay oladigan odamlar kerak.

Uchinchi muhim shaxsiy sifatlardan biri mas'uliyatlilik hisoblanadi, bu ish bo'yicha bog'liq bo'lgan odamlarda uning o'z vaqtida kelib, o'zining ishi bilan mashg'ul bo'lishi to'g'risida ishonch mavjud bo'lishi uchun kerakdir.

To'rtinchi sifat – bilimdonlik, katta miqdordagi mahsulotlar to'g'risida ma'lumotlar ola bilish va eng muhimi uni bajarish xohishining mavjudligi, unda keng ammo axborot texnologiyalarining barcha sohasi bo'yicha chuqur bo'lmagan bilimi bo'lishi lozim. Ko'p beriladigan savolar bo'yicha tushunchaga ega bo'lish va konsultatsiya olish mumkin bo'lgan ikkinchi bosqichdagi mutaxassislar guruhini bilishi lozim.

6.3. Axborot xavfsizligi insidentlariga javob qaytarishning asosiy bosqichlari

Axborot xafsizligida insident yuzaga kelishida ko'p hollarda kompleks va ko'p tomonlama muammolar sabab bo'ladi. Ushbu muammoning to'g'ri yechimi birinchi navbatda uni struktura komponentalariga dekompozisiya qilish va har bir komponent uchun kiruvchi va chiquvchi ma'lumotlarni o'rganib chiqishdir.

Insidentga javob qaytarishning asosiy bosqichlari quyidagilar:

1. Insident yuzaga kelishiga tayyor bo'lish. Tashkilot insident yuzaga kelish holatiga tayyor bo'lishi lozim (uning oqibatlarini kamaytirish uchun).
2. Insidentlarni o'rganib chiqish bo'yicha komissiya tuzish (CSIRT). Bu bosqich muhim bosqichlardan biri hisoblanadi va hamda insidentni tergov qilishni muvaffaqiyatli o'tishi ham bu bosqichga bog'liqdir.
3. Insidentni aniqlash - axborot xafsizligi insidentini identifikasiyasi.
4. Boshlang'ich javob qaytarish - birinchi darajali tergov ishlarini boshlanishi, asosiy voqealarni yozib olish, komissiya tuzilish, tergov olib borilishiga aloqador shaxslar aniqlanish. Qonunga xilof harakatlarni aniqlash.
5. Javob qaytarish strategiyasini shakllantirish. Strategiya ma'lum bo'lgan barcha faktlarga asoslanib quriladi. Kompaniyaning top-menedjeri tomonidan tasdiqlanadi. Strategiya shu bilan birga qanday harakatlar amalga oshirilishi kerakligini ham ko'rsatib o'tadi.

6. Insident tergovi - ma'lumotlarni tahlili va yig'ishi orqali olib boriladi. Barcha to'plangan ma'lumotlar o'rganib chiqib qachon bo'lgan, qayerda bo'lgan, kim tomondan qilingan harakatlar tekshiriladi.

7. Hisobot - to'laqonli hisobot o'z tarkibida tergov davomida topilgan ma'lumotlar bir joyga yig'ilib tushunarli tarzda bayon qilinganligi haqida ma'lumot beradi.

8. Yechim - himoya mexanizmlarini tashkil qilish va keyinchalik bunday vaziyatlar bo'lishini oldini olish.

Bo'lishi mumkin bo'lgan insidentlar.

Har bir insident boshqasidan farq qiladi va o'zgacha yechim talab qilishi mumkin. Shuning uchun ishchi guruh har bir holatga har hil yondashishi kerak. Bo'lishi mumkin bo'lgan insidentlar:

1. Serverni buzish.
2. Elektron pullarni o'g'irlash.
3. IP-telefoniyani buzish.
4. Tarmoq trafigi o'g'irlash.
5. Maxfiy ma'lumotlarni chiqib ketishi.
6. Ma'lumotlar yo'qolishi.
7. Maqsadga yo'naltirilgan virusli hujumlar.
8. Boshqa insidentlar.

Hozirgi kunda banklarning asosiy e'tibori axborot xavfsizligi insidentini boshqarishga qaratilgan. Buning asosiy sabablaridan biri masofaviy bank tizimlarida o'g'irliklar sodir etilishi ko'payib ketgani sabab bo'lmoqda. Axborot xavfsizligi insidentlari bank faoliyatidagi biznes jarayonlar buzilishiga, iqtisodiy mavqe'ga va ishonchni yo'qotishga jiddiy ta'sir o'tkazishi mumkin. Va hatto axborot xavfsizligidagi kichkina muammoalar ham yig'ilib katta buzilishga olib kelishi mumkin. Axborot xavfsizligi insidentlarini boshqarish tizimidan foydalanish va tadqiq etish bank hodimlari ish jarayonlarini boshqarish uchun imkoniyatlar yaratib beradi. Shuni asosida yetkaziladigan zarar kamayadi, tezda vaziyatni bartaraf etish imkoni bo'ladi.

O'z vaqtida insidentlarni aniqlash, uni paydo bo'lishiga javob qaytarish va keyinchalik takrorlanmasligini ko'rib chiqish kerak. Hozirgi kunda shunaqa standartlardan biri bu GOST R ISO/MEK TO 18044-2007 standarti «Informasionnaya texnologiY. Metodi i sredstva obespecheniya bezopasnosti. Menedjment insidentov informasionnoy bezopasnosti» (GOST 18044-2007)- axborot xavfsizligi insidentlariga bag'ishlangan asosiy standartlardan biri hisoblanadi. Axborot

xavfsizligi insidentlariga tayyorgarlik, tezkorlik ko'p hollarda yetkaziladigan zarar kamayishiga imkon beradi. Ko'p insidentlar vaqt o'tishi bilan paydo bo'ladi, buning oqibatida har xil yomon oqibatlar yuzaga keladi, shuning uchun ham axborot xavfsizligi xizmatlarining asosiy vazifalaridan biri shunday oqibatlarni tezda aniqlashdir.

To'g'ri tuzilgan va rejalashtirilgan insidentlarni boshqaruv usulida (GOST 18044-2007 standarti) quyidagilarni keltirish mumkin:

- optimal usullar asosida axborot xavfsizligi insidentlari identifikasiyasiga ruxsat berish va baholash;
- himoya choralariga mos ravishda axborot xavfsizligi insidentlari salbiy oqibatlari ta'sirini kamaytirish;
- axborot xavfsizligi insidentlaridan to'g'ri dars olish.

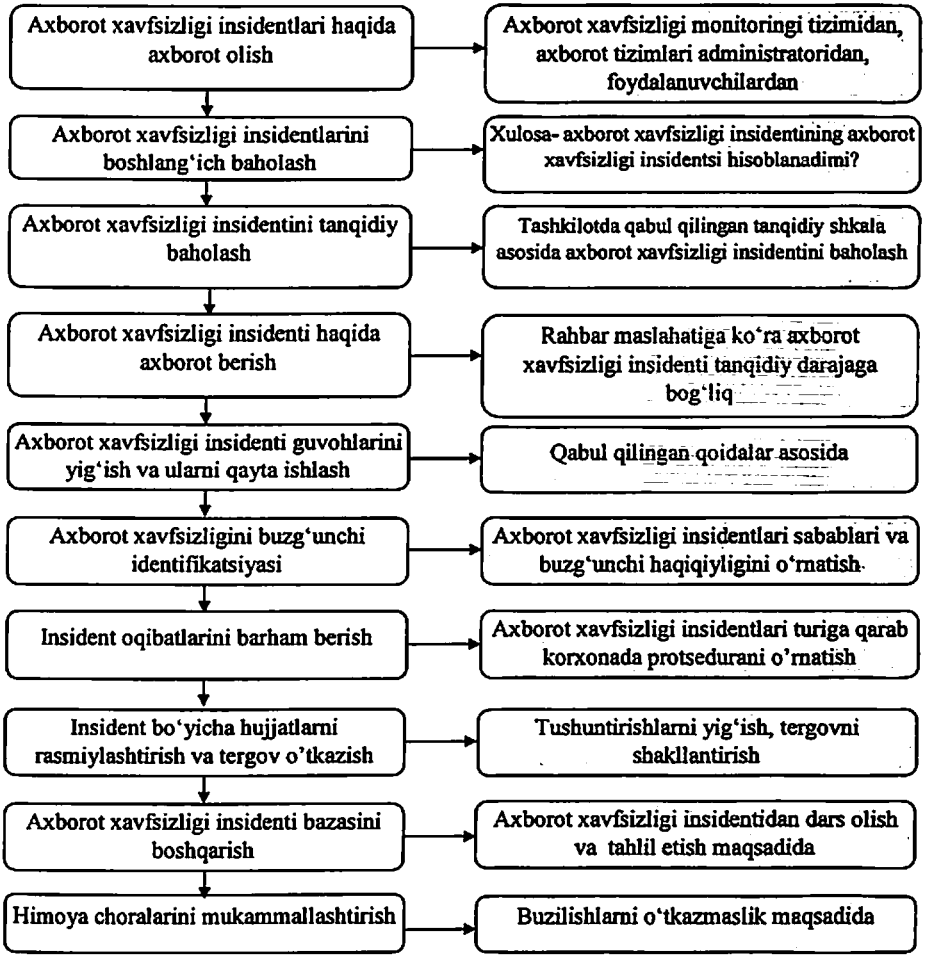
Barcha kerakli jarayonlarni ishga tushirgandan keyin, bank tizimi rejali va tizimli tekshiruvlar o'tkazib borishi zarur. Shu yo'l bilan axborot xafsizligi insidentlarini aniqlash osonlashadi. Umumiy holda insidentlarni aniqlash va ularga javob qaytarishni quyidagi algoritmda ko'rish mumkin (6.6-rasm).

Axborot xavfsizligi insidentlarida javob qaytarish prosedurasi insident turiga, uning tanqidiy darajasiga, bo'lishi mumkin bo'lgan zararlariga, tashkilot rahbariyati javobiga qarab turli xil bo'lishi mumkin.

Hozirgi kunda axborot xavfsizligi insidentlariga katta e'tibor qaratilmoqda. Tabiiy ravishda, hozirda bir qancha banklar moliyaviy yo'qotishlarga duchor bo'lmoqda. Faktlarni paydo bo'lish holatini nazorat etish uchun metodik tavsiyalar ishlab chiqarilgan. Banklar xavfsizlik xizmati va huquqni muhofaza qiluvchi tashkilotlar tomonidan axborot xavfsizligi insidentlarini tergov qilish vaqtida qallobchilik qilgan shaxslar jinoiy javobgarlikga tortilmoqda.

Intizomiy javobgarlik.

Tajribada axborot xavfsizligi insidentlari klassifikasiyasi ekspert usullar orqali, lekin odatda qoida bo'yicha turli mutaxassislar tomonidan amalga oshiriladi. Xuddi mana shu jarayonda tizimlilikni va insidentni klassifikasiyasi va kelajakda javob qaytarish uchun qaror qabul qilishda subyektivizmni kamaytirish darajasini oshirish zarur hisoblanadi.



6.6-rasm. Axborot xavfsizligi insidentlarida javob qaytarish va ularni aniqlash algoritmi

Bu esa o'z navbatida qoidalarni oldindan tayyorlab borish, o'qitish va har doim tekshiruvda saqlash bilan amalga oshiriladi. Ekspert yechim topishni matematik ko'rinishini qurilmaviy aniq bo'lmagan mantiq yordamida ifodalash mumkin, bunday usul bilan biz kerakli natijani aniq bo'lmagan holatlarda ham topish mumkin. Ekspert tajribasi asosida axborot xavfsizligi insidenti klassifikasiyasini mantiqiy-lingvistik modeli quriladi. Bunda u kiruvchi va chiquvchi mantiqiy lingvistik

qiymatlar bilan ifodalanadi va ular o‘zaro qandaydir evristik qoidalar bilan bog‘lanadi (2-jadval).

2-jadval

Axborot xavfsizligi insidenti klassifikasiyasini mantiqiy-lingvistik modeli

1.	“Agar<vaziyat 1> bo‘lsa unda <harakatni amalga oshir 1>”
2.	“Agar<vaziyat 2> bo‘lsa unda <harakatni amalga oshir 2>”.
....	.....
N	“Agar<vaziyat n> bo‘lsa unda <harakatni amalga oshir n>”.

Axborot xavfsizligi insidenti klassifikasiyasi amalga oshirilgandan so‘ng insidentga javob qaytarish harakati boshlanadi. Buning uchun bankda axborot xavfsizligi insidenti klassifikasiyasini aniqlangan algoritmi ma’lum bo‘lishi zarur. Bunday aniqlik daraja “hech qanday natijasiz” yoki “ahamiyatsiz” guruhlansa ham unga javob baribir bo‘lishi lozim.

Ma’lumotlar bazasini shakllantirish.

Axborot xavfsizligi insidentlariga javob qaytarishda mavjud faktorlar-bu axborot xavfsizligi insidentlari bazasiga mos keluvchi hujjatlarni to‘g‘ri yuritishdir. Bu o‘z navbatida materiallarni tekshirish uchun yig‘ish va birlashtirish imkonini beradi. Ogohlantiruvchi chora-tadbirlarni qo‘llashda axborot xavfsizligi insidentlariga javob qaytarish jarayonidagi asosiy maqsad negativ oqibatlarni kamaytirishdir. Shu bilan birga insident yopilgandan keyin ko‘riladigan chora tadbirlar quyidagilardir (xafsizlik siyosatini o‘zgaritish, yaxshi bo‘lmagan resusrlarni yopib qo‘yish va h.k).

Xodimlar bilan profilaktik ishlarni amalga oshirish quyidagilarni o‘z ichiga olishi mumkin:

- qoidabuzarga jazolarni qo‘llash;
- qoidabuzarga negativ imidj yaratish;
- foydalanuvchilarni o‘qitish va qo‘shimcha maslahatlar berish;
- axborot xavfsizligi talablariga rioya qiluvchi qo‘llanmalarni tarqatish;
- bank axborot xavfsizligi siyosatiga o‘zgartirishlar kiritish va h.k.

Umumiy holda axborot xavfsizligi insidentlarini boshqarish jarayonini tezkorligi va samaradorligi quyidagi faktorlarga bog'liq bo'ladi:

- jalb qilingan barcha sathlar koordinasiyalashtirilgan holda ishlashi;
- insident bilan bog'liq axborotni tahlili va olish imkoniyatlarini mavjudligi;
- olingan natijalarni to'g'riligi va tezkorligi.

6.4 Axborot xavfsizligi insidentlari sohasida o'qitish va xabardor etishni ta'minlash

Axborot xavfsizligi insidentlari sohasida o'qitish va xabardorlikni oshirish.

Axborot xavfsizligi insidentlarini boshqarish - nafaqat texnik vositalarni, balki xodimlarni ham o'z ichiga oladigan jarayondir, demak, bu jarayon tashkilotda ishlash uchun tegishli tayyorgarlikdan o'tgan va axborot xavfsizligi masalalaridan xabardor shaxslar tomonidan qo'llabquvvatlanishi lozim.

Tashkilotning barcha a'zolarining xabardorligi va ishtiroki axborot xavfsizligi hodisalarini boshqarishga tizimli yondashuvni muvaffaqiyatli ta'minlash uchun muhim. Foydalanuvchilar bu jarayonda ishtirok etishi lozim bo'lsa ham, agar ular axborot xavfsizligi insidentlarini boshqarishga tizimli yondashuvdan o'zlari va bo'linmalari qanday foyda ko'rishlari haqida xabardor bo'lmasalar bunday ishtirokning samaralilik ehtimoli kam bo'ladi. Axborot xavfsizligi insidentlarini boshqarishga tizimli yondashuvning eksluatasion samarasi va sifati bir qator omillarga, shu jumladan, insidentlar haqida xabar berish majburiyati, hisobot sifatida, foydalanishning osonligi, tezlik va o'qitishga bog'liq. Bu omillardan ayrimlari foydalanuvchilar axborot xavfsizligi insidentlarini boshqarishning ahamiyatini bilishlarini va insidentlar haqida xabar berishga tayyorligini nazarda tutadi.

Axborot xavfsizligi insidentlarini boshqarishning roli o'qitish va axborot xavfsizligi masalalarida xabardorlikni ta'minlash umumiy dasturining bir qismi sifatida faol qo'llab-quvvatlanmog'i lozim. Xabardorlikni ta'minlash dasturi va tegishli material barcha xodimlar, shu jumladan, ya'ni xodimlar, uchinchi tashkilotlar va pudratchilarning foydalanuvchilari uchun foydalana olinadigan bo'lishi lozim. Kontakt posiziyasi (KP), axborot xavfsizligi insidentlariga ta'sir etish xizmati (AXITX) a'zolari, zarurat bo'lganda esa - axborot xavfsizligi uchun

mas'ul xodimlar va ma'murlar uchun maxsus o'qitish dasturi bo'lishi lozim. Insidentlarni boshqarish jarayonida bevosita ishtirok etuvchi har bir guruh a'zosi uchun uning axborot xavfsizligi insidentini boshqarish sxemasidagi ishtirokining turi, darajasi va hajmidan kelib chiqqan holda har xil tayyorgarlik darajasi kerak bo'lishi mumkin.

Xabardorlikni ta'minlash bo'yicha tezkor majlis quyidagilarni qamrab olishi lozim:

1. tashkilot va uning xodimlari uchun axborot xavfsizligi insidentlarini boshqarishga tizimli yondashuvdan kelib chiqadigan afzalliklar;
2. axborot xavfsizligi insidentlarini boshqarish sxemasining ishlash asosari, shu jumladan uning harakatlari doirasi va axborot xavfsizligi insidentlari, hodisalari va zaifliklarini boshqarish bo'yicha ishlar texnologiyasi;
3. axborot xavfsizligi hodisalari, insidentlari va zaifliklari haqidagi hisobotlar usullari;
4. insident to'g'risida mavjud ma'lumotlar va axborot xavfsizligi hodisalari/insidentlari/zaifliklari ma'lumotlar omborida olingan ma'lumotlar;
5. manbalar maxfiyligini ta'minlash mexanizmlari (zarurat bo'lganda);
6. sxema xizmatining darajalari bo'yicha kelishuv;
7. faoliyat natijalari haqida hisobot yuritish - manbalar qanday shartlarda xabardor qilinadi;
8. oshkor qilmaslik to'g'risidagi kelishuvlardan kelib chiqadigan har qanday cheklovlar;
9. axborot xavfsizligi insidentlarini boshqarish tashkilotining vakolatlari va uning hisobot beruvchi liniyasi;
10. axborot xavfsizligi insidentlarini boshqarish tizimi hisobotlarini oluvchilar.

Ayrim xollarda axborot xavfsizligi insidentlarini boshqarish bo'yicha xabardorlikni ta'minlash haqidagi ma'lumotni boshqa o'qitish dasturlariga (masalan, xodimlar uchun kirish dasturlari yoki axborot xavfsizligi masalalari bo'yicha xabardorlikni ta'minlashning umumiy korporativ dasturlari) maxsus kiritish maqsadga muvofiqdir. Xabardorlikni ta'minlashga bunday yondashuv xodimlarning ayrim guruhlari bilan bog'liq kimmatli ma'lumotlarni taqdim qilishi va o'qitish dasturining samaradorligini yaxshilashi mumkin.

Axborot xavfsizligi insidentlarini boshqarish tizimini ishga tushirishdan oldin barcha tegishli xodimlar axborot xavfsizligi insidentlarini aniqlash va hisobot berish proseduralari biilan tanishtirmog'i, maxsus tanlangan xodimlar esa keyingi jarayonlar bo'yicha yaxshi xabardor qilingan bo'lishi lozim. Keyin xabardorlikni ta'minlash bo'yicha muntazam instruktaj va tayyorgarlik kurslari o'tkaziladi. Tayyorgarlik jarayonida KP guruhi va AXITX a'zolari, shuningdek, axborot xavfsizligi uchun mas'ullar va ma'murlar uchun maxsus mashqlar va nazorat o'tkazilishi lozim.

Bundan tashqari, o'qitish va xabardorlikni oshirish dasturlari axborot xavfsizligi hodisalari/insidentlari va zaifliklari hisobotoni berish va qayta ishlashda sustkashlikni minimallashtirish maqsadida axborot xavfsizligi insidentlarini boshqarishni amalga oshiradigan xodimlar tomonidan «kaynok liniya» ning yaratilishi va ishlashi bilan to'ldirilishi lozim.

Axborot xavfsizligi insidentlari sohasida hodisalarni aniqlash.

Axborot xavfsizligi voqealari bevosita biron-bir xavotirga sabab bo'ladigan va texnik, jismoniy va proseduraviy xarakterga ega bo'lgan vaziyatni sezgan shaxs yoki shaxslar tomonidan aniqlanishi mumkin. Aniqlash, masalan, yong'in/tutun detektorlari yoki qo'riqlash signalizasiyasi tomonidan oldindan belgilab qo'yilgan joylarga ogohlantirish signallari uzatish orqali (inson tomonidan ma'lum bir xatti-harakatlar amalga oshirilishi uchun) amalga oshirilishi mumkin. Axborot xavfsizligining texnik insidentlari (anomal tarmoq faolligi, xizmatning ishdan chiqishiga mo'ljallangan hujumlar, ruxsat berilmagan ma'lumotni qo'lga kiritishga urinish, zararli kodni yuklash va hokazo) avtomatik aniqlanishi mumkin, masalan, bular nazorat yozuvlari tahlili qurilmalari, tarmoqlararo ekranlar, hujumlarni aniqlash tizimlari, zararli kodlarni aniqlashning instrumental vositalari (shu jumladan antivirus dasturlari) tomonidan yuboriladigan ogohlantirish signallari bo'lishi mumkin, har safar signallar bu qurilmalarning oldindan belgilangan parametrlari tomonidan faollashtiriladi.

Axborot xavfsizligi hodisalarini aniqlashning ehtimoliy manbalariga quyidagilar kiradi:

- foydalanuvchilar;
- rahbariyat va xavfsizlik xizmati rahbarlari;
- mijozlar;

- axborot texnologiyalari bo'limi, shu jumladan Tarmoqni ekspluatasiya qilish markazi va Xavfsizlik operasion markazi (2-daraja qo'llabquvvatlanishi orqali);
- axborot texnologiyalari yordamchi xizmatlari (1-daraja qo'llab quvvatlanishi orqali);
- boshqariladigan xizmatlar provayderlari (shu jumladan internet provaydelar va telekommunikasiyalar xizmatlari provayderlari);
- AXITX;
- har kungi ishi davomida anomaliyalarni aniqlashi mumkin bo'lgan boshqa bo'linmalar va xodimlar;
- OAV (gazetalar, televideniye va hokazo);
- veb-saytlar (axborot xavfsizligi bo'yicha veb-saytlar, xavfsizlikni tadqiq kiluvchilar veb-saytlari va hokazo).

Axborot xavfsizligi insidentlari sohasida hodisalar hisobotini yuritish.

Axborot xavfsizligi hodisasini aniqlash manbaidan qat'iy nazar, noodatiy narsaga e'tibor qaratgan yoki avtomatik vositalar tomonidan xabardor qilingan shaxs aniqlash va hisobot jarayonini boshlash uchun mas'ul bo'ladi. Bu shaxs tashkilotda doimiy yoki xizmat shartnomasi asosida ishlayotgan har qanday xodim bo'lishi mumkin.

Bu vakil birinchi navbatda KP va rahbariyatning e'tiborini jalb qilish maqsadida axborot xavfsizligi insidentlarini boshqarish sxemalarida belgilangan proseduralarga rioya qilishi va axborot xavfsizligi hodisalari haqidagi hisobot shakllarini ishlatishi lozim. Demak, barcha xodimlar axborot xavfsizligi ehtimoliy hodisalari haqida xabardor qilish masalalariga tegishli tavsiyalar, shu jumladan, hisobot shakllari bilan tanishgan bo'lishi va axborot xavfsizligi hodisasining har bir yuzaga kelish holati haqida xabardor qilinishi lozim bo'lgan xodimlarni tanishi mumkin. Bunga axborot xavfsizligi hodisalari haqidagi hisobotlar shakllari va har bir insident haqida ogohlantirilishi lozim bo'lgan shaxslar haqidagi ma'lumotlar kiradi (barcha xodimlar xech bo'lmaganda hisobot shakllari haqida xabardor qilinishi lozim, bu ularning axborot xavfsizligi insidentlarini boshqarish sxemasini tushunishlariga yordam beradi).

Shuni ta'kidlash lozimki, eshitilishdan himoya qilingan stasionar, simsiz yoki mobil telefon xavfsiz emas. Maxfiy axborot bilan ishlayotganda qo'shimcha himoya choralari ko'rilishi lozim.

Quyidagi ma'lumotlar insidentlarni kuzatish tizimlarida qayd shakllari uchun asos bo'lib xizmat qilishi mumkin:

- aniqlangan vaqt/sana;
- kuzatuvlar;
- bog'lanish uchun ma'lumotlar (majburiy emas).

To'ldirilgan shakl (qog'ozda yoki elektron pochta orqali yoki veb-shakllar orqali taqdim qilingan) AXITX xodimlari tomonidan faqat axborot xavfsizligi insidentlarini insidentlarni kuzatish tizimlarida qayddan o'tkazish paytida ishlatilishi lozim. Ehtimoliy/sodir bo'lib o'tgan/aniqlangan axborot xavfsizligi hodisalari haqida ma'lumotlar/hisobotlar olish muhim.

Axborot xavfsizligi hodisalarini (ehtimoliy insidentlarini) kuzatish iloji boricha avtomatlashtirilgan dasturlar tomonidan amalga oshirilishi lozim. Axborot tizimlarini ko'llash xodimlarni o'rnatilgan proseduralar va nazorat ruyxatlariga rioya qilishga majburlash uchun muhim. Shuningdek, «kim nima va kachon kilganligini» hamda axborot xavfsizligi hodisasi (ehtimoliy insidenti) paytida hato tufayli tushirib qoldirilishi mumkin bo'lgan tafsilotlarni kuzatib borish foydalidir.

Konkret axborot xavfsizligi hodisasini qayta ishlash bu hodisa nimadan iboratligiga hamda olib kelishi mumkin bo'lgan oqibatlar va ta'sirlarga bog'liq. Ko'pchilik uchun hodisani qayta ishlash usuli haqida qaror qabul qilish ularning vakolatlariga kirmaydi. Shuning uchun axborot xavfsizligi hodisasi haqida xabar berayotgan xodim shaklni shunday to'ldirishi kerakki, unda o'sha paytda ma'lum bo'lgan iloji boricha ko'proq axborot aks etishi kerak. Zarurat bo'lganda xodim o'z rahbari bilan bog'lanadi. Bu shakllarni xavfsiz usul bilan tegishli KPga (sutkasiga 24 soat, xaftasiga 7 kun ishlaydigan) uzatishi kerak, xabarning nushasi esa mas'ul AXITX ga uzatilishi kerak. Axborot xavfsizligi hodisasi haqidagi hisobot namunasi D ilovada keltirilgan.

AXITX elektron pochta, telefon, faks orqali yuborilgan barcha hisobotlar uchun mas'ul xodim yoki vakilni tayinlashi kerak. Bu mas'uliyat xizmat xodimlari orasida har xafta o'tib turishi mumkin. Xizmatning tayinlangan xodimi vaziyatni baholaydi hamda mas'ul va manfaatdor tomonlarni xabardor qilish uchun, shuningdek, axborot xavfsizligi insidentlarini bartaraf qilish uchun zarur choralarni ko'radi.

Shuni alohida ta'kidlash lozimki, hisobot shakllarini to'ldirishda nafaqat mazmunning aniqligi, balki vaqtida to'ldirilishi ham juda muhim. Shuningdek axborot xavfsizligi hodisasi haqidagi hisobotni yuborishni uning mazmuniga aniqlik kiritish maqsadida kechga qoldirib ham bo'lmaydi. Agar xabar beruvchi hisobot shaklining biron-bir

qismidagi ma'lumotga ishonchi komil bo'lmasa, bu qismni belgilab qo'yish kerak va ma'lumotni keyinchalik aniqlashtirib jo'natish lozim. Shuni ham tan olish lozimki, elektron ayrim elektron hisobot mexanizmlari (masalan, elektron pochta) o'zi ham xujumga nishon bilishi mumkin.

Odatiy ishlatiladigan elektron hisobot mexanizmlari (masalan, elektron pochta) bilan muammolar mavjud bo'lganda yoki muammolar mavjudligiga shubha bo'lgan taqdirda, shuningdek, tizimga hujum bo'lganda va hisobotlar vakolati bo'lmagan shaxslar tomonidan o'qilganda alternativ aloqa vositalari ishlatilishi lozim. Alternativ aloqa vositalariga xodimlar, telefonlar yoki matnli xabarlar kirishi mumkin. Bunday alternativ aloqa vositalari tergovning ilk bosqichlarida, axborot xavfsizligi hodisasi axborot xavfsizligi insidenti sifatida tasniflanishi aniq bo'lganda, ayniqsa, bunday axborot xavfsizligi insidenti muhim deb sanaladigan paytda ishlatilishi lozim.

Axborot xavfsizligi insidenti tezda yolg'on risk sifatida aniqlanishi yoki qoniqarli yechimga olib kelinishi mumkin. Bunday xollarda hisobot shakllarini to'ldirish hamda KP va AXITX ning mahalliy rahbariyatiga qayd qilish maqsadida, ya'ni axborot xavfsizligi hodisalari/insidentlari/zaifliklari ma'lumotlar omboriga kiritilishi uchun jo'natish lozim. Bunday holda axborot xavfsizligi hodisasi yopilgani haqida xabar beruvchi shaxs axborot xavfsizligi insidentlari haqidagi hisobot shakllarini to'ldirish uchun talab qilinadigan ma'lumotlarni uzatishi mumkin - bunda axborot xavfsizligi insidenti haqidagi hisobot shakli to'ldirib, tegishli organlarga jo'natilishi lozim.

Asosiy xulosalar

Axborot xavfsizligi insidentlariga tezkor javob qaytarish o'z ichiga texnik chora – tadbirlarni, kriminal belgili ma'lumotlar to'liqligini ta'minlash va bu ma'lumotlarning tergov qilish ehtimolligi, hamda insidentdan ko'riluvchi zararni kamaytiruvchi va huquqni himoya qiluvchi organlar uchun hujjatlar tarkibidan va tashkiliy chora – tadbirlardan iborat.

Axborot xavfsizligi insidentlarini boshqarish jarayoni faqatgina ruxsat berish emas, balki ularni tahlil qilish, ruxsat effiktivligini ta'minlash ham muhim. Ishlab chiqilgan rejalarni ishchi muhitning qo'llab – quvvatlashiga testlash va modifikatsilash kerak. Agarda tahlil davrida insidentning o'xshash nusxalari aniqlansa, maqbul harakatlar takrorlanadi. Agarda tizim xatoliklari aniqlansa belgilangan rejalar natija bermasa, unda tayyorgarlik bosqichiga o'tiladi.

- Oltin – MCHS, IIV, avariya xizmatlari va organlari tomonidan qo'llab – quvvatlovchi, yuqori menejment tashkilotlari,
- Kumush – xavf – xatarlarni va biznesdagi uzulishlar boshqarish xizmati.
- Bronza – AT va Axborot xavfsizligi markazlari, kadrlarni qo'llab quvvatlash, yuristlar, texnik xavfsizlik va huquqni muhofaza qilish organlari.

Insidentlarga javob qaytarish – bu dinamik jarayon hisoblanadi. Uning ayrim bosqichlari parallel holda bajariladi, boshqalari esa ketma-ketlikda, ya'ni keyingi bosqich oldingi bosqich natijalariga bog'liq bo'lgan holda bajariladi.

Insidentni tekshirish ishlari qolgan xavf-xatarlarni baholash prosedurasi va kelgusi ishlar uchun amaliy jihatdan foyda chiqarish bilan yakunlanadi.

Jahon amaliyotiga muvofiq ayrim eng yaxshi prinsiplarni shakllantiramiz, qaysiki bu prinsiplarga amal qilgan tashkilot axborot xavfsizligi insidentlariga javob qaytarishning samarali siyosati bilan ta'minlanadi.

Nazorat uchun savollar

1. Texnik chora va tashkiliy chorani bir biridan farqi nimada?
2. Hujum insidentlari harakatlarining umumiy algoritmlari.
3. Axborot xavfsizligi insidentlarini boshqaruvchanligi deganda nimani tushunasiz?
4. IBM Security QRadar insidentlar ekspertizasi qanday ekspertiza hisoblanadi?
5. Axborot xavfsizligi insidentlarini aniqlashning texnik vositalari aytib bering.
6. Axborot xavfsizligi insidentlarini aniqlashning tizimlari.
7. Insidentlarga javob qaytarish proseduralari deganda nima tushunasiz?
8. Insidentning hayotiy sikli nima anglatadi?
9. Insidentga javob qaytarishni amalga oshirish prinsiplari.
10. Insidentlarni darajalanishi tushuntiri bering.
11. Insidentga axborot ta'sir o'tkazish qanday amalga oshiriladi?
12. Insidentga axborot ta'sir o'tkazish deganda nimani tushunasiz?

ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Prezidenti 2017 yil 7 fevraldagi PF-4947-son «O'zbekiston Respublikasini yanada rivojlantirish bo'yicha Harakatlar strategiyasi to'g'risida» gi Farmoni

2. Зефиров С.Л., Щербакова А.Ю., Управление инцидентами кибербезопасности: уч.пособие / Пенза: Изд-во ПГУ, 2012.

3. Н.Г.Милославская, М.Ю.Сенаторов, А.И.Толстой, Управление инцидентами информационной безопасности и непрерывностью бизнеса, Горячая линия – Телеком, Москва, 2015.

4. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».

5. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».

6. O'z DSt ISO/IEC 27035:2015 «Методы обеспечения безопасности. Управление инцидентами информационной безопасности»

7. Зефиров С.Л. Менеджмент инцидентов информационной безопасности: учебное пособие. – Пенза: Изд-во ПГУ, 2008.

8. Нестеров С.А. Основы информационной безопасности: уч.пособие / СПб.: Лань, 2017.

9. Жукова М.Н. Управление информационной безопасностью. Ч.2. Управление инцидентами информационной безопасности: уч.пособие / Красноярск: Сиб.гос.аэрокосмич. ун-т, 2012.

10. International Standard ISO/IEC 27035-2:2016(E) «Information technology — Security techniques — Information security incident management —Part 2: Guidelines to plan and prepare for incident response»

11. ISO/IEC 27037:2012 «Information technology. Security techniques. Guidelines for identification, collection and/or acquisition and preservation of digital evidence»

12. Paul Cichonski, Tom Millar, Tom Grance, Karen Scanfone, NIST. Computer Security Incident Handling Guide/Recommendations of the National Institute of Standards and Technology/ Special Publication 800-61/Revision 2, National Institute of Standards and Technology (NIST), 2012.

13. David R.Miller, Shon Harris, Allen A.Harper, Stephen VanDyke, Chris Blask, Security Information and Event Management Implementation, // the McGraw-Hill Companies, 2011. ISBN: 978-0-07-170108-2.

14. Завгородний В.И., Комплексная защита информации в компьютерных системах: уч.пособие // М.: Логос, 2010.

15. Кочнев В.Ф., Титов Е.В., Филиппов С.А., Обнаружение нелегального пользователя компьютерной системы: уч.пособие // М.: МИИТ, 2003.

16. Курило А.П., Зефиров С.Л., Голованов В.Б., Аудит информационной безопасности // М.: Изд.гр. БДЦ Пресс, 2006

17. Россинская Е.Р., Усов А.И., Судебная компьютерно-техническая экспертиза. Практическая юриспруденция. Судебная экспертиза. М.: Право и закон, 2001.

18. Варганов Д.С., Состояние и перспективы развития технологии защиты программных продуктов //Безопасность информационных технологий, №1, 2008.

19. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф., Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004.

20. Альтерман Б.Д., Дрожжинов В.И., Моисеенка Г.Е., Обеспечение непрерывности деятельности организации в нештатных ситуациях // Jet Info, 2003.

21. Давыдова Н.Н. Криминалистические классификации преступлений и методик их расследования// Н.Н. Давыдова. – Саратов: СГАП, 2009.

22. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов / – М.: ООО «Издательство Машиностроение», 2009.

Интернет-ресурсы:

1. CERT Coordination Center www.cert.org
2. 6 Steps to Incident Handling www.giac.org/resources/whitepaper/network/17.php
3. Bibliography of Computer Security Incident Handling Documents, by Klaus-Peter Kossakowski, DFN-CERT (Germany) www.cert.dfn.de/eng/pre99papers/certbib.html
4. NIST Incident Handling Information http://csrc.nist.gov/topics/inchand.html

BELGILAR VA QISQARTMALAR

ACL – Access Control List
CBR- Case-based reasoning
CCTV –Slosed Circuit Television
CGI - Common Gateway Interface
CPU - Central Processing Unit
DAS - Directly Attached Storage
DNS - Domain Name System
ICMP - Internet Control Message Protocol
IR – Internet Protocol Address
ICQ - I seek you
IOS - iPhone OS
GPS - Global Positioning System
GSM - Groupe Special Mobile
FTK - Forensic Toolkit
FTP - File Transfer Protocol
HTTP – Hyper Text Transfer Protocol
HPA – Host Protocol Area
LIR - Local Internet registry
NAS - Network Attached Storage
NIC - Network Interface Card
NGI - Next Generation Internet
ODD - Optical Disk Drive
PIN - Personal Identification Number
RAID - Redundant Array of Inexpensive Disks
RICAS - Real-time Intelligence Crime Analytics System
RIR - Regional Internet Registry
RIPE - Réseaux IP Européens (Network Coordination Centre)
TLS – Transport Layer Security
TCP – Transmission Control Protocol
URL - Uniform Resource Locator
WLAN - Wireless Local Area Network
AX- Axborot xavfsizligi
AXBT - Axborot xavfsizligini boshqarish tizimi
ATX - Axborot texnologiyalari xizmati
AXX - Axborot xavfsizligi xizmati
INX - Ichki nazorat xizmati
HX - Huquqiy xizmat

IXX - Iqtisodiy xavfsizlik xizmati

XBX - Xavflarni boshqarish xizmati

PBX - Personalni boshqarish xizmati

BJE - Biznes jarayonlar egasi

AXIBS - Axborot xavfsizligi insidentlari boshqarish siyosati

AXIQHG - Axborot xavfsizligi insidentiga qarshi harakat guruhi

SOC-Axborot xavfsizligi insidentlari reaksiya va monitoring markazi

CBR - boshqarish jarayonini avtomatlashtirish vositalari

MBBT – ma'lumotlar bazasini boshqarish tizimlari

AXMT – Axborot xavfsizligi menedjment tizimi

AXIJQ - axborot xavfsizligi insidentlariga javob qaytarish

AXIJQG -Axborot xavfsizligi insidentlariga javob qaytarish guruhi

KP - kontakt posiziyasi

AXITX - axborot xavfsizligi insidentlariga ta'sir etish xizmati

TERMINLAR LUG'ATI

ACL (Access Control List) - obektga (dasturga, jarayonga yoki faylga) kim va nima kira olishi mumkinligini va qaysi subektga (foydalanuvchi, foydalanuvchilar guruhi) ishlashi taqiqlangan yoki taqiqlanmaganligini belgilaydigan erkin foydalanishni boshqarish ro'yxati.

CBR (Case Based Reasonin) – pretsedentga asoslangan fikrlash - keng ma'noda ma'lum yechimlar asosida yangi muammolarni hal qilish usuli hisoblanadi.

DAS (Directly Attached Storage) - serverlarga bevosita ulangan ma'lumotlarni saqlash tizimlari.

DNS (Domain Name System), *DNS*, domen nomlari xizmati - domen nomi tizimi, shuningdek, domen nomining rezolyutsiyasini amalga oshiruvchi server tizimi (DNS-serverlar).

DOS (DenialofService) hujum - "xizmat ko'rsatishni rad etish" ko'rinishidagi kompyuter tarmog'i, kompyuter yoki axborot tizimiga hujum.

EnCase - kompyuter ekspertizasining barcha bosqichlari uchun texnologiya va dasturiy ta'minot.

IP-adres (Internet Protocol Address) – TCP/IP protokollar to'plamiga asoslangan kompyuter tarmog'idagi noyob tarmoq manzili tugunlari.

FTK (Forensic Toolkit) - kompyuter ekspertizasi sohasidagi standart.

FTP (File Transfer Protocol) – fayllarni uzatish protokoli - TCP-tarmog'ida fayllar uzatish uchun standart protokol.

Proxy server - manzilni translyatsiya qilish deb ataladigan jarayon xavfsizlik devori bilan bog'liq IP manzilini o'zgartirish uchun ishlatiladigan vositachi server (xavfsizlik devori).

RAID (Redundant Array of Inexpensive Disks) - ishonchsiz komponentlardan ishonchli qurilmani hosil qilish tipik injenerlik masalasini yechimi.

Rootkit - tizimda tajovuzkor yoki zararli dastur mavjudligini izini yashiruvchi dastur yoki dasturlar majmua.

TCP (Transmission Control Protocol) – uzatishni boshqarish protokoli, Internet ma'lumotlarini uzatishning asosiy protokollaridan biri, ma'lumotlar uzatilishini boshqaradi. TCP va IP protokollariga ega tarmoqlar va quyi tarmoqlarga TCP/IP tarmoqlari deyiladi.

TLS (Transport Layer Security) – internet tarmog'ida tugunlar orasidagi ma'lumotlarni himoyalangan holda uzatishni ta'minlaydigan transport darajasi himoya protokoli.

Wireshark - tarmoq trafigi analizatori.

Whois - domen yoki uning IP- manzili kimga qayd qilinganligi haqida server mijozga ma'lumot uzatishi mumkin bo'lgan protokol.

Himoyaning apparat vositalari - axborotni ruxsatsiz kirish, nusxalash, o'g'irlash yoki o'zgartirishdan himoya qilish uchun mo'ljallangan mexanik, elektron, optik, lazerli, radio, radar va boshqa qurilmalar, tizimlar va tuzilmalar.

Autentifikatsiya (*Authentication*) - taqdim etilgan identifikator bo'yicha sub'ektni kirish uchun ruxsat etilganligini tekshirish; haqiqiyligini tasdiqlash; belgilangan identifikator sifatida odatda **login** va **bank (to'lov) karta paroli,** kartochka - mijozlar tomonidan to'lash talab qilinganda to'lov va boshqa hujjatlarni tuzish uchun vositalar tashkil qiladi.

Autsorsing xizmatlari (*outsourcing,outer-source-usin- tashqi manba va/yoki resurslardan foydalanish*) – buyurtmachi kompaniya qator ichki xizmatlarini va/yoki ichki servislarini, shuningdek uning dasturiy mahsulotlari, ilovalari, apparat va infrastruktura qismlaridan foydalanish asosida, tasgqi pudratchiga o'tkazish.

Billing tizimi – hisob-kitobning avtomatlashgan tizimi.

Bot (*Boot*) - avtomatik ravishda va/yoki muntazam foydalanuvchi sifatida bir xil interfeyslar orqali biron-bir amalni oldindan belgilangan jadvalga muvofiq bajaradigan maxsus dastur.

Brandmauer *(Firewall)* - tarmoqni boshqa tizim va tarmoqlardan apparat-dasturiy vositalar nazorati yordamida, xavfsizlikka tahdidlardan himoya qilish usuli/vositasi.

Brauzer (*Brawser*), veb_brauzer, internet_brauzer, veb_klient – veb_sahifa va boshqa tarmoq axborot resurslarini ko'rish; foydalanuvchining shaxsiy kompyuterida o'rnatilgan, tarmoq orqali web_server bilan bog'lanish, undan ma'lumot so'rash va undan olish (odatda HTML formatida) uchun dastur, uni veb-sahifadagi shaklda ko'rsatadi va qayta ishlaydi.

Virmeyker - kompyuter viruslari ishlab chiqarishchi programmist.

Virtual olam (*Virtua lreality, VR*, sun'iy borliq) - insonga sezgi organlari: ko'riish, eshitish, hid bilish, teri sezish va boshqalar orqali texnik vositalar (obekt va subekt) yordamida yaratilgan dunyo.Virtual borliq ta'sir o'tkazishni va unga javobni imitatsiya qiladi.

Veb-server - bu serverda o'rnatilgan va HTTP yoki HTTPS protokoli yordamida **veb-sayt** bilan foydalanuvchi brauzeri o'rtasida aloqa o'rnatadigan dastur.

Veb-sahifa - foydalanuvchiga uzatiladigan (odatda HTML tilida) axborotning brauzerdagi natijasi.

Veb-sayt - "o'rgimchak, tarmoq" va *sayt* - "joy", "joy, segment, tarmoqning bir qismi" - mantiqiy jihatdan veb-sahifalar to'plami, jumladan server kontenti joylashuvi.

Zararli dastur, *virus, malware* - axborotni blokirovkalash, o'zgartirish yoki nusxalashga olib keladigan, kompyuter, kompyuter tizimi yoki ularning tarmoqlarini buzishga sabab bo'ladigan kompyuter dasturi. Zararli dasturlar turlari: virus, qurt, troyan, mantiqiy bomba, eksploit, rutkit.

Global navigatsiya tizimi - makon va zamon ma'lumotlarini aniqlash va uni huquqni muhofaza qilish organlari tomonidan qabul qilishni tashkil etish imkonini beruvchi usullar, dasturiy va apparat vositalar to'plami.

Defeys - (*deface* - buzmoq, o'zgartirmoq) - asosiy (yoki boshqa muhim) sahifa ikkinchisi bilan – odatda ko'zga tashlanih holatida (reklama, ogohlantirish, xavf, internet) almashinishi olib keladigan xakerlik hujumi. Ko'pincha, saytning qolgan qismiga kirish taqiqlanadi yoki eski sayt mazmuni to'liq o'chiriladi.

Domen - noyob domen nomi bilan belgilanadigan Internet domen nomlari ierarxik shajarasining qismi.

Qayta tiklash jurnali - ma'lumotlar bazasini yoki faylni tiklash qobiliyatini ta'minlaydigan jurnal. Bazadagi har qanday o'zgarishlar haqida o'rnatilgan vaqtidan buyongi ma'lumotlarni o'z ichiga oladi, ma'lumotlar ishonchliligi va zaxira nusxasi mavjudligini ko'rsatadi.

Tergich (*Dialers*) - pullik telefon liniyalari suiste'mol qilish orqali firibgarlik turi.

Zombi tarmog'i, botnet - yagona markazdan boshqariladigan troyan dasturi turi bilan zazarlangan kompyuterlar guruhi; odatda, bunday tarmoq tuzilmasi keraksiz boshqarish aloqalari bilan tuzilgan; spam yuborish, hujumlar uyushtirish, trafikning haqiqiy manbalarini yashirish va boshqa vazifalarni bajarish uchun ishlatiladi; birdan o'n minglab kompyuterlarga ega bo'lishi mumkin.

Axborot tizimi - ma'lumotlar bazalarida va axborot texnologiyalarida va uni qayta ishlashni ta'minlaydigan texnik

vositalardagi ma'lumotlar to'plami; axborot tizimi ko'pincha "kompyuter, kompyuter tizimi, ularning tarmog'i" deb atash mumkin.

Sun'iy intellekt - aqlli mashinalar, ayniqsa aqlli kompyuter dasturlari yaratishning ilm-fan va texnologiyasi; aqlli tizimlarning an'anaviy ravishda insonning imtiyozi deb hisoblangan ijodiy funktsiyalarni amalga oshirish qobiliyati.

Insayder (*Insider*) - keng omma foydala olmaydigan axborotdan foydalanish imkoniga ega bir guruh odamlar a'zosi. Termin sir bilan bog'liq bo'lgan kontekstda yashirin, yoki biron-bir boshqa nodavlat ommaviy axborot yoki bilimga nisbatan ishlatiladi: insayder - faqat ushbu guruhda mavjud ma'lumotlarga ega guruh a'zosi.

Insident - ruxsatsiz kirishni ta'minlash yoki kompyuter tizimiga hujum qilish uchun qilingan urinish.

AT (Axborot texnologiyalari) - kompyuterlar, kompyuter dasturlari, kompyuter tarmoqlari bilan bog'liq bilimlar va iqtisodiyotining sohasi; aloqa sohasi bilan chambarchas bog'liq.

Kontsentrator, *tarmoq kontsentratori, hub* - 2-bosqichda ishlaydigan freymlarni tarqalishini (takrorlashni) amalga oshiruvchi tarmoq aloqa qurilmasi, kompyuterlarni kompyuter tarmog'ining bir qismida ulash uchun ishlatiladi; kommutatordan farqli o'laroq, har bir olingan freym bir emas, balki barcha portlarga yuboriladi; odatda, konfiguratsiya qilinmaydi va nazorat qilinmaydi.

Log, log-fayl - kompyuterning voqea jurnali; ma'lum bir axborot tizimi yoki dasturiga ta'luqli hodisalarning yozuvlari bilan fayl yoki ma'lumotlar bazasi.

Login, *foydalanuvchi nomi* – foydalanuvchining belgili identifikatori; ko'pincha autentifikatsiya qilish uchun parol bilan birga ishlatiladi.

Mantiqiy bomba - dasturning turi (ba'zan zararli deb tan olingan), uning maqsadi o'rnatilgan kompyuterda eng nozik ma'lumotlarni yo'q qilishdir; oldindan aniqlangan shartlarni bajarmagan yoki amalga oshira olmaganligi sababli paydo bo'lgan.

Marshrutizator, *router, ruter* - (odatda IP protokoli tomonidan) paketlarni marshrutlovchi 3-darajada ishlovchi vosita, turli tarmoq qatlamlariga ulash uchun ishlatiladi.

Ruxsatsiz kirish (RK) - belgilangan tartibni buzgan holda axborot tizimiga yoki kompyuter ma'lumotlariga kirish; bu atama "noqonuniy

kirish" huquqiy atamasidan farqli o'laroq, texnik hisoblanadi, lekin deyarli bir xil ma'noni anglatadi.

Yangilanish, *patch* - alohida kompyuter dasturini yoki butun axborot tizimini funktsionalligini oshirish yoki noto'g'ri xatolar uchun yangilash uchun mo'ljallangan o'rnatish ko'rsatmalariga ega dastur yoki ma'lumotlar to'plami; mustaqil qiymatga ega emas, faqat yangilangan dastur bilan ishlatiladi; yangilanishlar, odatda, yangilanayotgan dastur ishlab chiqarilgan kompaniya tomonidan ishlab chiqariladi, lekin ba'zan boshqa shaxslar tomonidan yaratilgan yangilanishlar ham uchrab turadi.

Tezkor-qidiruv tadbirlari (TQT) – ma'lum taktik masalalarni yechishga qaratilgan o'zaro aloqador harakatlar tizimidan iborat operativ- qidiruv faoliyatining muhim elementi.

PIN-kod - (Personal Identification Number- shaxsiy identifikatsiya nomeri) - parol analogi. Operatsiyani avtorizatsiya qilish vaqtida u karta egasining terminalga (bankomatga) kirishi uchun parol sifatida va so'rovni raqamli imzolash uchun maxfiy kalit sifatida ishlatiladi. PIN-kod kredit va shunga o'xshash kartalar uchun taqdim etilgan; karta egasiga ruxsat berish uchun ishlatiladi.

Dasturiy ta'minot, DT, *software*, *soft* - EHM dasturlari uchun umumlashtirilgan nom; termin dasturiy va apparat (*yumshoq* va *qattiq*) qismlarni solishtirishda qo'llaniladi.

Kommunikatsiya protokoli, almashinuv protokoli - turli dasturlar, qurilmalar, axborot tizimlari orasidagi ma'lumotlarni almashish qoidalari to'plami; odatda texnik standart bilan aniqlanadi; bitta protokolning ikkita dasturiga rioya qilish ularning muvofiqligi uchun zarur shartdir.

Registratorlar - Internetda IP-manzillarni ajratish va qayd qilish bilan shug'ullanuvchi tashkilot (IP Registry).

Referer (to refer - jo'natmoq, yo'naltirmoq) referal dastur doirasida daromad olish maqsadida foydalanuvchilarni ma'lum internet-resurslariga yo'naltiruvchi odam.

Tarmoq kartasi, *tarmoq platasi, NIC* (network interface card) - muayyan interfeys orqali tarmoq bilan o'zaro ta'sirlashuv vazifalarini bajaradigan kompyuter platasi (qurilma); Tarmoq simini yoki antennani ulash uchun bir yoki bir nechta tashqi konnektorga ega.

Skimming (*skimming*) – maxsus qurilma yordamida karta ma'lumotlarini o'g'irlash. Buzg'unchilar kartaning magnit chizig'idan barcha ma'lumotlarni ko'chirib olishadi. Skimming PIN-kodni mini-kamera yoki katakchalar yordamida topish imkonini beradi.

Sniffer yoki *trafik analizatori* (*to sniff - hidlamoq*) - tarmoq trafigini (o'ziniki yoki birovnikini) qo'lga olish va tahlil qilish dasturi yoki qurilmasi.

Ijtimoiy muhandislik - axborot xavfsizligi tizimini xizmat xodimlari va foydalanuvchilar bilan aloqada olingan ma'lumotlar yordamida chetlab o'tish, xiyla va nayranglarni qo'llash orqali ularning ishlarini chalkashtish.

Spam – electron pochta orqali nomaqbul, ommaviy jo'natmalar, ICQ, SMS va boshqa elektron aloqa vositalarida kamroq uchraydi

Spamer - spamni yuborish yoki spam jo'natish (manzillarni to'plash, jo'natish uchun dasturlarni yaratish, spam tarqatilgan resurslarni saqlash va boshqalar) bilan shug'ullanadigan professional shaxs.

Steganografiya - ochiq axborot massivlarida maxfiy ma'lumotlarni yashirish uchun matematik usullarni o'rganadigan fanning sohasi.

Trafik, *tarmoq trafigi* - raqamli aloqa liniyasi orqali uzatiladigan ma'lumotlarning miqdori bit yoki baytlarda o'lchanadi; kamroq holatlarda atama axborot oqimini anglatadi, ya'ni bir vaqtning birligiga etkazilgan ma'lumotlarning miqdori, bit/s yoki bayt/s; tarmoq orqali uzatiladigan freymlar, paketlar, datagramlarning tarkibi.

Troyan dasturi, *trojan* - yashirincha yoki niqoblanib foydalanuvchining kompyuteridagi dasturiy ta'minotiga foydalanuvchining (operatorning) manfaatlariga va xohishiga mos bo'lmagan xatti-harakatlarni bajarish uchun ruxsatsiz o'rnatiladigan zararli dastur turi.

Fayl (file) - disk yoki boshqa kompyuter vositalarining nomlangan maydoni; nomi, boshqa atributlari va alohida sarlavhasi hamda alohida fayl tanasiga ega; fayl tizimida axborotni saqlash birligi hisoblanadi.

Fishing (*phishing*) - onlayn firibgarlik turi, jabrlanuvchining shaxsiy ma'lumotlarini (bank kartasi, parol, shaxsiy identifikatsiya ma'lumotlari) olishga asoslangan. Bunda xuddi ishonchli tashkilotlar (bank, provayderlar, davlat organlari) tomonidan jo'natilgan qalbaki xat va veb-saytlardan foydalanadi.

Haker - juda yuqori malakali kompyuter mutaxassisi; tajovuz qiluvchi kompyuter ma'lumotlariga, odatda tarmoq orqali ruxsatsiz kirishni amalga oshiradi.

Hesh , hesh-summa yoki bir tomonlama hesh funktsiyasi - maxsus algoritm yordamida fayl mazmunidan hisoblanuvchi uzun sonlar qatori. Xesh summasi checksumga o'xshaydi, biroq u bir muhim farqga ega: bu bir tomonlama funksiyadir. Ya'ni, faylni xesh funktsiyasini hisoblash oson, lekin ma'lum bir hesh funktsiyasiga mos faylni tanlash mumkin emas.

Gruming - bolalarni Internetdan aldash uchun tajovuzkorlarning harakatlarini belgilaydi. Bu usul metodikaning asosiy mohiyatini anglatadigan "g'amxo'rlik" yoki "g'amxo'rlik" deb tarjima qilingan inglizcha so'zlashtiruvchi terimdan kelib chiqadi: bolaga g'amxo'rlik hissi yaratish va keyingi jinoyatlarni sodir etish uchun barqaror psixologik aloqani o'rnatish.

Raqamli suv belgisi (RSB) – multimedia fayllarining mualliflik huquqini himoyalash dasturi. Odatda raqamli suv belgilar ko'rinmas bo'ladi. Biroq, RSB tasvir yoki videoda ko'rinishi mumkin. Odatda bu ma'lumot muallifni identifikatsiya qiluvchi matn yoki logotip bo'lishi mumkin.

Ekvayring - o'ziga bank kartochkalari orqali amalga oshiriladigan operatsiyalar bo'yicha savdo korxonalari (xizmatlarni) bilan hisob-kitoblarni amalga oshirish va ushbu kredit tashkilotining mijozlari bo'lmagan bank kartochkalarini egalariga naqd pul berish bo'yicha operatsiyalarni amalga oshiradigan kredit tashkilotlari faoliyati.

Ekvayver- ekvayveringni amalga oshiradigan kredit tashkiloti.

Eksployt - kompyuter dasturi, dasturiy ta'minot kodining bir qismi yoki dasturiy zaifliklardan foydalanadigan va kompyuter tizimiga hujum qilish uchun ishlatiladigan buyruqlar ketma-ketligi.

Eskapizm - psixologik travmalar, murakkab ish faoliyati, xavfli yashash muhiti, "asabiy ishda" faoliyat yurutmaydigan insonlar bilan yaxshi munosabatlar o'rnata olmaslik tufayli kelib chiqadigan doimiy va kuchli stress sababli paydo bo'ladigan holatlarda real olamdan qochish.

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, 2021

"Hujum insidentlari va unga reaksiya"

5330300- Axborot xavfsizligi ta'lim yo'nalishi bo'yicha bakalavriatura talabalari uchun o'quv qo'llanma.

"AXT" kafedrasi majlisida
ko'rib chiqildi va nashr etishga ruxsat etildi.
2020 yil 19 may
17 - sonli bayonnoma

"AX" fakulteti UK majlisida
ko'rib chiqildi va nashr etishga ruxsat etildi.
2020 yil 27 may
9 - sonli bayonnoma

Muhammad al-Xorazmiy nomidagi
TATU uslubiy Kengashi majlisida
ko'rib chiqildi va nashr etishga ruxsat etildi.
2020 yil 23 iyun
9(134) - sonli bayonnoma

Tuzuvchilar:

Sh.R.Gulomov
F.B.Botirov
Z.I.Azizova

Taqrizchilar:

M.B.Zaynutdinova

B.A.Allaberganov

Mas'ul muharrir:

A.A.Ganiyev

Musahhih:

S.X.Abdullaeva

SH.R. GULOMOV, F.B. BOTIROV, Z.I. AZIZOVA

HUJUM INSIDENTLARI VA UNGA REAKSIYA

Nashr uchun mas'ul: B. Mavlonov

Muharrir: U. Yunusov

Badiiy muharrir: F. Sobirov

Dizayner-sahifalovchi: L. Abdullayev

Nashriyot ro'yxat raqami № 1043191. 24.09.2021-y.
Bichimi 60x84 1/16 Offset qog'ozi.
Times New Roman garniturasi.
Shartli bosma tabog'i 10,25. Nashr hisob tabog'i 4,2.
Adadi 100 nusxada. Buyurtma № 10-12.

1940

100000, Toshkent shahri, Mirzo Ulug'bek tumani,
M.Ismoiliy ko'chasi 1-G uy.

«ZUXRA BARAKA BIZNES» MChJ bosmaxonasida chop etildi.
Toshkent shahri Bunyodkor shoh ko'chasi 27 A–uy.