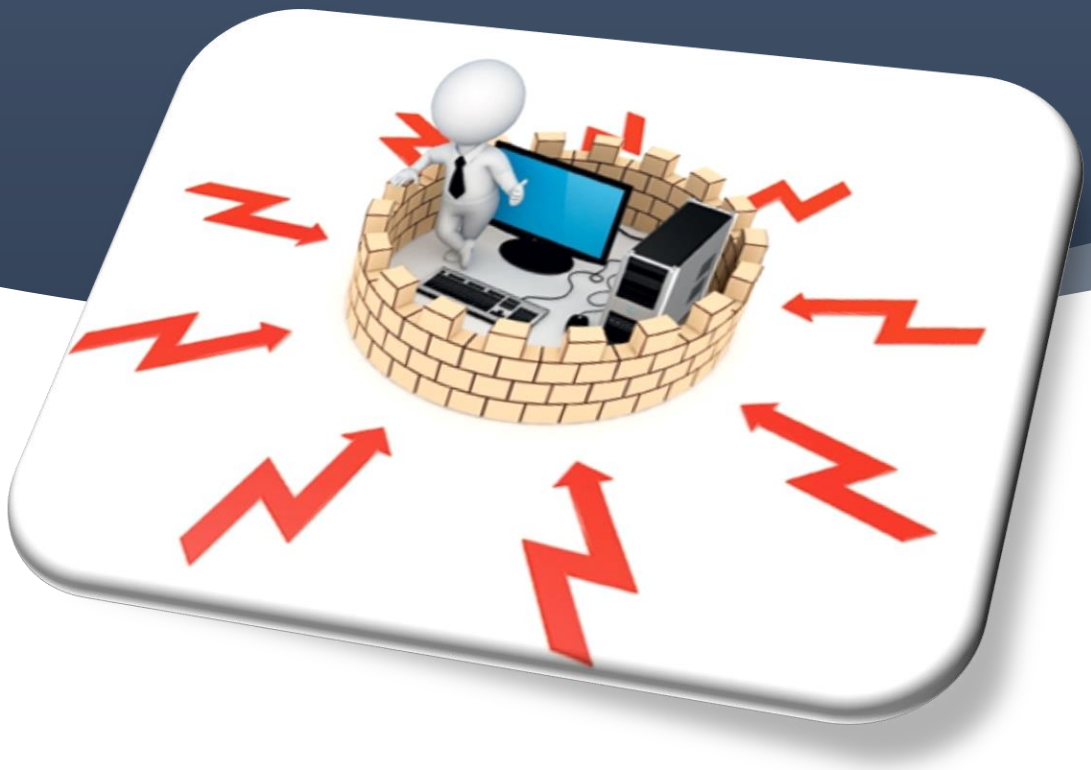
ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ
МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

’ҳужум инцидентлари ва унга реакция” ФАНИ БЎЙИЧА

ЎҚУВ-УСЛУБИЙ МАЖМУА



ТОШКЕНТ-2019

Мазкур ўқув-услубий мажмуа Олий ва ўрта махсус таълим вазирлигининг 201__ йил “___” _____ даги _____-сонли буйруғи билан тасдиқланган ўқув режа ва дастур асосида тайёрланди.

Тузувчи: Муҳаммад ал-Хоразмий номидаги ТАТУ доценти, PhD, Ш.Р. Ғуломов

Ўқув -услубий мажмуа (Муҳаммад ал-Хоразмий номидаги ТАТУ кенгашининг 2018 йил “____”_____даги ___-сонли қарори билан тасдиққа тавсия қилинган.

МУНДАРИЖА

I. СИЛАБУС

2018/2019 ўқув йили

<table>
<tr><th colspan="6">Фаннинг қисқача тавсифи</th></tr>
<tr><td>ОТМ номи ва манзили</td><td colspan="2">Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети</td><td colspan="3">Амир Темур 108, Тошкент</td></tr>
<tr><td>Факультет ва кафедра</td><td colspan="2">Ахборот хавфсизлиги</td><td colspan="3">Ахборот хавфсизлигини таъминлаш</td></tr>
<tr><td>Таълим йўналиши:</td><td>5330500</td><td colspan="4">Компьютер инжиниринги (“Ахборот хавфсизлиги”)</td></tr>
<tr><td>Фаннинг профессор ўқитувчилари хақида маълумот</td><td>Маъруза: Ғуломов Ш.Р.
Амалиёт: Насруллаев Н.Б.</td><td>e-mail:

Телефон:</td><td colspan="3">sherzod.gulomov@rambler.ru

+998712386509</td></tr>
<tr><td>Фаннинг жадвали ва аудитория №. 205 Д</td><td>Ахборот хавфсизлигини таъминлаш кафедрасига тегишли хоналар</td><td>Фанни ўқитиш муддати:</td><td colspan="3">21.01.2019-06.04.2019</td></tr>
<tr><td rowspan="2">Фанга ажратилган соатлар</td><td colspan="4">Аудитория машғулотлари</td><td rowspan="2">Мустақил таълим:</td><td rowspan="2">36</td></tr>
<tr><td>Маъруза:</td><td>36</td><td>Амалиёт</td><td>36</td></tr>
<tr><td>Бошқа фанлар билан боғлиқлиги (талаблар):</td><td colspan="6">“Ахборот хавфсизлиги”, “Ахборот тизимларини аудитлаш”, “Бузиш ва ҳимоялаш принциплари” фанлари билан ўзаро боғликликда ўрганилади.</td></tr>
<tr><th colspan="7">Фаннинг мазмуни</th></tr>
<tr><td>Фаннинг долзарблиги ва мазмуни:</td><td colspan="6">Фаннинг долзарблиги –компьютер тармоқлари ва тизимларида инцидентларга қарши жавоб қайтариш усуллари ва воситалари, уларни аниқлаш муҳим аҳамият касб этади. Шу мезонларни ҳисобга олган ҳолда фаннинг ҳозирги ахборот асрида долзарблигини аниқлаш мумкин.
Фаннинг мазмуни – ахборот хавфсизлиги</td></tr>
</table>

	инцидентларини бошқариш тизими, ахборот хавфсизлиги инцидентларини қайта ишлаш ва аниқлаш, ахборот хавфсизлиги инцидентларига жавоб қайтаришни ҳаёт даври ва ахборот хавфсизлиги инцидентлари соҳасида ўқитиш ва хабардор этишни таъминлаш усулларини ўрганишдир.
Фан бўйича талабанинг малакасига қўйиладиган талаблар	– ахборот хавфсизлиги инцидентлари ҳақида ***тасаввурга эга бўлиши***; – ахборот хавфсизлиги инцидентларини бошқариш тизими ҳақида ***билмларга эга бўлиши;*** – ахборот хавфсизлиги инцидентларини бошқариш жараёни ҳақида ***тасаввурга эга бўлиши;*** – ахборот хавфсизлиги инцидентларини идентификациялаш ва ***баҳолаш мезонларини билиши;*** – ахборот хавфсизлиги инцидентларига жавоб қайтариш гуруҳларини шакиллантириш бўйича ***тасаввурга эга бўлиш;*** – суқилиб киришлар усулларини ***таҳлил эта олиши;*** – ахборот хавфсизлиги инцидентлари соҳасида ўқитиш ва хабардор этишни таъминлаш бўйича ***билим ва кўникмаларига эга бўлиши керак;*** – ахборот хавфсизлиги инцидентларида даллиларни сақлаш ва тергов этиш усулларини билиши ва ***улардан фойдалана олиши;*** – ахборот хавфсизлиги инцидентлари режаси ва ҳисоботларини ишлаб чиқиш ҳақидаги ***кўникмаларига эга бўлиши керак.***

Фанида машғулот мавзулари ва соатлари бўйича тақсимланиши:

Умумий ва ўқув ишлари турлари бўйича ҳажми.

8 - СЕМЕСТР

Ўқув машғулоти соатларини ҳафталар бўйича тақсимоти

№	Маш-ғулот тури	Жами	Ҳафталар											
			1	2	3	4	5	6	7	8	9	10	11	12
1	Маъруза	36	2	4	4	2	4	2	2	4	4	2	4	2
2	Амалиёт	36	2	4	4	2	4	2	4	2	2	4	2	4
3	Мустақил иш	36	4	3	4	2	3	2	2	2	3	4	3	4
	Жами	**108**	**8**	**11**	**12**	**6**	**11**	**6**	**8**	**8**	**9**	**10**	**9**	**10**

МАЪРУЗА МАШҒУЛОТЛАР МАЗМУНИ (8-семестр)

№	Маърузалар	Ажратилган соат
1.	Кириш. Ахборот хавфсизлиги инцидентларини бошқаришда норматив базалар.	2
2.	Ахборот хавфсизлиги инцидентларини бошқариш тизими.	4
3.	Ахборот хавфсизлиги инцидентларини бошқариш сиёсати. Ахборот хавфсизлиги инцидентларини бошқариш жараёни.	4
4.	Ахборот хавфсизлиги инцидентларини идентификациялаш ва баҳолаш мезонлари.	2
5.	Ахборот хавфсизлиги инцидентларини қайта ишлаш ва аниқлаш.	4
6.	Ахборот хавфсизлиги инцидентларига жавоб қайтариш.	2
7.	Ахборот хавфсизлиги инцидентларига жавоб қайтаришни ҳаёт даври процедураси.	2
8.	Ахборот хавфсизлиги инцидентларига жавоб қайтариш гурухи.	4
9.	Ахборот хавфсизлиги инцидентларини бошқариш дастурлари.	4
10.	Ахборот хавфсизлиги инцидентлари соҳасида ўқитиш ва хабардор этишни таъминлаш.	2
11.	Ахборот хавфсизлиги инцидентларини тергов этиш. Ахборот хавфсизлиги инцидентлари даллиларини сақлаш.	4
12.	Ахборот хавфсизлиги инцидентларини назорат этувчи воситаларнинг таҳлили.	2
	Жами:	**36**

АМАЛИЙ МАШҒУЛОТЛАР МАЗМУНИ (8-семестр)

№	Мавзулар	Ажратилган соат
1.	Ахборот хавфсизлиги инцидентларини бошқаришни қуриш жараёнлари.	2
2.	Ахборот хавфсизлиги инцидентларини гуруҳларга ажратиш.	4
3.	Жараёнлар ўртасида ролларни тақсимлаш ва инцидентни бошқариш жараёнидаги ходимларни аниқлаш.	4
4.	Ахборот хавфсизлиги инцидентларининг тергови.	2
5.	Ахборот хавфсизлиги инцидентларини тергов қилиш жараёнидаги қаршиликлар.	4
6.	Ахборот хавфсизлиги инцидентлари терговида гуруҳлар тузилмаси.	2
7.	Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг асосий босқичлари.	4
8.	Ахборот хавфсизлиги инцидентларига жавоб қайтариш процедурасининг ҳаётий даври.	2

9.	Ахборот хавфсизлиги инцидентларига жавоб қайтариш алгоритми.	2
10.	Корхонада ахборот хавфсизлиги инцидентларини тергов қилиш ва уларни баҳолаш усуллари.	4
11.	Ахборот хавфсизлиги соҳасида жиноятларнинг криминал таснифи.	2
12.	Ахборот хавфсизлиги инцидентларини прецедентли тахлил қилиш асосида тадқиқ этиш.	4
	Жами:	**36**

МУСТАҚИЛ ИШЛАР МАВЗУСИ

№	Мавзулар	Ажратилган соат
1.	Ахборот хавфсизлиги инцидентлари мақсади ва вазифаси.	4
2.	Ахборот хавфсизлиги инцидентлари сиёсатини қуриш.	3
3.	Ахборот хавфсизлиги инцидентлари бошқариш тизимларини таҳлил этиш усуллари.	2
4.	Ахборот хавфсизлиги инцидентлари жараёнини бошқариш воситалари.	4
5.	Ахборот хавфсизлиги инцидентлари аниқлаш ва баҳолаш.	3
6.	Ахборот хавфсизлиги инцидентларида экспертиза жараёнини ўтказиш.	4
7.	Ахборот хавфсизлиги инцидентларига жавоб қайтариш ҳаёт даври процедураси таҳлил этиш.	2
8.	Ахборот хавфсизлиги инцидентларига жавоб қайтариш гурухларини шакллантириш.	2
9.	Ахборот хавфсизлиги инцидентларини бошқариш дастурлари таҳлил этиш ва дастурий модуллар ишлаб чиқиш усуллари.	2
10.	Ахборот хавфсизлиги инцидентлари ҳақида хабардор этиш механизмини тадқиқи.	4
11.	Ахборот хавфсизлиги инцидентларини тергов қилиш жараёнидаги қаршиликларни бартараф этиш усуллари.	2
12.	Криминалистик жиноятлар ва уларнинг классификацияси.	4
	Жами:	**36**

ТАЛАБАЛАРНИ БАҲОЛАШ МЕЗОНЛАРИ:

№	Кўрсатгичлар	ОН баллари		
		макс	1-ОН	2-ОН
1	Дарсларга қатнашганлик ва ўзлаштириши даражаси.	15	0-7	0-8
2	Мустақил таълим топшириқларини бажарилиш ва ўзлаштириши даражаси.	10	0-5	0-5
3	Ёзма назорат иши натижалари бўйича	15	0-8	0-7

	Жами ОН баллари	40	0-20	0-20
№	Кўрсатгичлар	ЖН баллари		
		макс	1-ОН	2-ОН
1	Дарсларга қ тнашганлик ва ўзлаштириши даражаси.	10	0-5	0-5
2	Мустақил таълим топшириқларини бажарилиш ва ўзлаштириши даражаси.	10	0-5	0-5
3	Оғзаки савол-жавоблар ва бошқа назорат турлари натижалари бўйича	10	0-5	0-5
	Жами ЖН баллари	**30**	**0-15**	**0-15**
№	Кўрса гичлар	ЯН баллари		
		макс	Ўзгариш оралиғи	
1	Фан бўйича якуний ёзма иш назорати	**30**	**0-30**	
Жами:		**100**	**0-100**	

Адабиёт-лар

1. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия–Телеком, 2014. – 170 с.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.
3. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
4. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

II. ФАННИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

“SWOT-таҳлил” методи.

Методнинг мақсади: мавжуд назарий билимлар ва амалий тажрибаларни таҳлил қилиш, таққослаш орқали муаммони ҳал этиш йўлларни топишга, билимларни мустаҳкамлаш, такрорлаш, баҳолашга, мустақил, танқидий фикрлашни, ностандарт тафаккурни шакллантиришга хизмат қилади.

Намуна: Ахборот хавфсизлиги инцидентларини бартараф этиш усул ва воситалари учун SWOT таҳлилини ушбу жадвалда туширинг.

S	Ахборот хавфсизлиги инцидентларини бартараф этиш усул ва воситалари	Компьютер тизимларида ахборот алмашиниш ҳолатини тезда минимал ахборот хавфсизлиги хавф-хатарлари билан нормал иш ҳолатига қайтариш.
W	Ахборот хавфсизлиги инцидентларини бартараф этиш усул ва воситалари	Компьютер тармоқларида бўлиши мумкин бўлган ҳужум ва таҳдидларни махсус дастурий-аппарат воситаларисиз бартараф эта олмайди.
O	Ахборот хавфсизлиги инцидентларини бартараф этиш усул ва воситалари	Кирувчи ва чиқувчи ахборотни тўлақонли назорат этиш, персонални бошқариш хизмати, ахборот хавфсизлиги инцидентларини олидини олишни

		ҳужжатлаштириш.
Т	Ахборот хавфсизлиги инцидентларини бартараф этиш усул ва воситалари	OSI моделидаги ҳама сатҳларни назорат этиш имкониятига эга эмас. Бунинг учун махсус дастурий воситадан фойдаланиш талаб этилади.

"Хулосалаш" (Rezyume, Veyer) методи

Методнинг мақсади: Бу метод мураккаб, кўптармоқли, мумкин қадар, муаммоли характеридаги мавзуларни ўрганишга қаратилган. Методнинг моҳияти шундан иборатки, бунда мавзунинг турли тармоқлари бўйича бир хил ахборот берилади ва айни пайтда, уларнинг ҳар бири алоҳида аспектларда муҳокама этилади. Масалан, муаммо ижобий ва салбий томонлари, афзаллик, фазилат ва камчиликлари, фойда ва зарарлари бўйича ўрганилади. Бу интерфаол метод танқидий, таҳлилий, аниқ мантиқий фикрлашни муваффақиятли ривожлантиришга ҳамда ўқувчиларнинг мустақил ғоялари, фикрларини ёзма ва оғзаки шаклда тизимли баён этиш, ҳимоя қилишга имконият яратади. “Хулосалаш” методидан маъруза машғулотларида индивидуал ва жуфтликлардаги иш шаклида, амалий ва семинар машғулотларида кичик гуруҳлардаги иш шаклида мавзу юзасидан билимларни мустаҳкамлаш, таҳлили қилиш ва таққослаш мақсадида фойдаланиш мумкин.

Методни амалга ошириш тартиби:

5-6 кишидан иборат кичик гуруҳларга тренер-ўқитувчи иштирокчиларни ажратилади;

тренинг мақсади, ҳар бир гуруҳга умумий муаммони таҳлил қилиниши зарур бўлган қисмлари туширилган тарқатма материалларни тарқатади;

ҳар бир гуруҳ ўзига берилган муаммони атрофлича таҳлил қилиб, ўз мулоҳазаларини тавсия этилаётган схема бўйича тарқатмага ёзма баён қилади;

навбатдаги босқичда барча гуруҳлар ўз тақдимотларини ўтказадилар. Шундан сўнг, тренер томонидан таҳлиллар умумлаштирилади ва мавзу якунланади.

Намуна:

NGNқурилмалари					
MSAN		**Медиашлюз**		**NetNumen**	
афзаллиги	камчилиги	афзаллиги	камчилиги	афзаллиги	камчилиги
Хулоса:					

“Кейс-стади” методи

«Кейс-стади» - инглизча сўз бўлиб, («case» – аниқ вазият, инцидент, «study» – ўрганмоқ, таҳлил қилмоқ) аниқ вазиятларни ўрганиш, таҳлил қилиш асосида ўқитишни амалга оширишга қаратилган метод ҳисобланади. Мазкур метод дастлаб 1921 йил Гарвард университетида амалий вазиятлардан иқтисодий бошқарув фанларини ўрганишда фойдаланиш тартибида қўлланилган.Кейсда очиқ ахборотлардан ёки аниқ воқеа-инцидентдан вазият сифатида таҳлил учун фойдаланиш мумкин. Кейс ҳаракатлари ўз ичига қуйидагиларни қамраб олади: Ким (Who), Қачон (When), Қаерда (Where), Нима учун (Why), Қандай/ Қанақа (How), Нима-натижа (What).

“Кейс методи” ни амалга ошириш босқичлари

Иш Босқичлари	**Фаолият шакли ва мазмуни**
1-босқич: Кейс ва унинг ахборот таъминоти билан таништириш	якка тартибдаги аудио-визуал иш; кейс билан танишиш(матнли, аудио ёки медиа шаклда); ахборотни умумлаштириш; ахборот таҳлили; муаммоларни аниқлаш
2-босқич: Кейсни аниқлаштириш ва ўқув топшириғни белгилаш	индивидуал ва гуруҳда ишлаш; муаммоларни долзарблик иерархиясини аниқлаш; асосий муаммоли вазиятни белгилаш
3-босқич: Кейсдаги асосий муаммони таҳлил этиш орқали ўқув топшириғининг ечимини излаш, ҳал этиш йўлларини ишлаб чиқиш	индивидуал ва гуруҳда ишлаш; муқобил ечим йўлларини ишлаб чиқиш; ҳар бир ечимнинг имкониятлари ва тўсиқларни таҳлил қилиш; муқобил ечимларни танлаш

4-босқич: Кейс ечимини ечимини шакллантириш ва асослаш, тақдимот.	якка ва гуруҳда ишлаш; муқобил вариантларни амалда қўллаш имкониятларини асослаш; ижодий-лойиҳа тақдимотини тайёрлаш; якуний хулоса ва вазият ечимининг амалий аспектларини ёритиш

Кейс. Ахборот хавфсизлиги инцидентларини гуруҳларга ажратиш. Талаба ахборот хавфсизлиги инцидентларини гуруҳларга ажратди ва унинг натижасида инсайдер маълумотларини таҳлил этишда хатолик юз берди.

Кейсни бажариш босқчилари ва топшириқлар:

- Кейсдаги муаммони келтириб чиқарган асосий сабабларни белгиланг(индивидуал ва кичик гуруҳда).
- Хатоликни бартараф этувчи ишлар кетма-кетлигини белгиланг (жуфтликлардаги иш).

«ФСМУ» методи

Технологиянинг мақсади: Мазкур технология иштирокчилардаги умумий фикрлардан хусусий хулосалар чиқариш, таққослаш, қиёслаш орқали ахборотни ўзлаштириш, хулосалаш, шунингдек, мустақил ижодий фикрлаш кўникмаларини шакллантиришга хизмат қилади. Мазкур технологиядан маъруза машғулотларида, мустаҳкамлашда, ўтилган мавзуни сўрашда, уйга вазифа беришда ҳамда амалий машғулот натижаларини таҳлил этишда фойдаланиш тавсия этилади.

Технологияни амалга ошириш тартиби:

- қатнашчиларга мавзуга оид бўлган якуний хулоса ёки ғоя таклиф этилади;

- ҳар бир иштирокчига ФСМУ технологиясининг босқичлари ёзилган қоғозлари тарқатилади:

- иштирокчиларнинг муносабатлари индивидуал ёки гуруҳий тартибда тақдимот қилинади.

ФСМУ таҳлили қатнашчиларда касбий-назарий билимларни амалий машқлар ва мавжуд тажрибалар асосида тезроқ ва муваффақиятли ўзлаштирилишига асос бўлади.

Намуна.

Фикр: “Ахборот хавфсизлиги инцидентларининг терговини амалга ошириш.

Топшириқ: Мазкур фикрга нисбатан муносабатингизни ФСМУ орқали таҳлил қилинг. Ахборот хавфсизлиги инцидентларининг терговини амалга оширишда эхтимоллик назариясидан фойдаланиш мақсадга мувофиқ саналади, чунки ҳар бир заифлик нуқталарида энг кўп ҳужум амалга оширадиганини танлаш муҳим ҳисобланади. Мисол сифатида DDOS ҳужумларни келтириш мумкин. Хулоса қилиб айтганда DDOS ҳужумларни минималлаштириш имконияти пайдо бўлади.

“Ассесмент” методи

Методнинг мақсади: мазкур метод таълим олувчиларнинг билим даражасини баҳолаш, назорат қилиш, ўзлаштириш кўрсаткичи ва амалий кўникмаларини текширишга йўналтирилган. Мазкур техника орқали таълим олувчиларнинг билиш фаолияти турли йўналишлар (тест, амалий кўникмалар, муаммоли вазиятлар машқи, қиёсий таҳлил, симптомларни аниқлаш) бўйича ташҳис қилинади ва баҳоланади.

Методни амалга ошириш тартиби:

“Ассесмент” лардан маъруза машғулотларида талабаларнинг ёки қатнашчиларнинг мавжуд билим даражасини ўрганишда, янги маълумотларни баён қилишда, семинар, амалий машғулотларда эса мавзу ёки маълумотларни ўзлаштириш даражасини баҳолаш, шунингдек, ўз-ўзини баҳолаш мақсадида индивидуал шаклда фойдаланиш тавсия этилади. Шунингдек, ўқитувчининг

ижодий ёндашуви ҳамда ўқув мақсадларидан келиб чиқиб, ассесментга қўшимча топшириқларни киритиш мумкин.

Намуна. Ҳар бир катакдаги тўғри жавоб 5 балл ёки 1-5 балгача баҳоланиши мумкин.

Тест

- 1. Инцидент аломатлари неччи турга бўлинади?
- A.3
- B.2
- C. 6

Қиёсий таҳлил

- Инцидент ва хавф-хатарни фарқи.

Тушунча таҳлили

- “Инцидентга жавоб қайтариш алгоритми.

Амалий кўникма

- Инцидентни бартараф этувчи дастурий восита яратилсин.

“Инсерт” методи

Методнинг мақсади: Мазкур метод ўқувчиларда янги ахборотлар тизимини қабул қилиш ва билмларни ўзлаштирилишини енгиллаштириш мақсадида қўлланилади, шунингдек, бу метод ўқувчилар учун хотира машқи вазифасини ҳам ўтайди.

Методни амалга ошириш тартиби:

- ўқитувчи машғулотга қадар мавзунинг асосий тушунчалари мазмуни ёритилган инпут-матнни тарқатма ёки тақдимот кўринишида тайёрлайди;
- янги мавзу моҳиятини ёритувчи матн таълим олувчиларга тарқатилади ёки тақдимот кўринишида намойиш этилади;
- таълим олувчилар индивидуал тарзда матн билан танишиб чиқиб, ўз шахсий қарашларини махсус белгилар орқали ифодалайдилар. Матн билан ишлашда талабалар ёки қатнашчиларга қуйидаги махсус белгилардан фойдаланиш тавсия этилади:

Белгилар	**1-матн**	**2-матн**	**3-матн**
“V” – таниш маълумот.			
“?” – мазкур маълумотни тушунмадим, изоҳ			

керак.			
“+” бу маълумот мен учун янгилик.			
“– ” бу фикр ёки мазкур маълумотга қаршиман?			

Белгиланган вақт якунлангач, таълим олувчилар учун нотаниш ва тушунарсиз бўлган маълумотлар ўқитувчи томонидан таҳлил қилиниб, изоҳланади, уларнинг моҳияти тўлиқ ёритилади. Саволларга жавоб берилади ва машғулот якунланади.

“Тушунчалар таҳлили” методи

Методнинг мақсади: мазкур метод талабалар ёки қатнашчиларни мавзу буйича таянч тушунчаларни ўзлаштириш даражасини аниқлаш, ўз билимларини мустақил равишда текшириш, баҳолаш, шунингдек, янги мавзу буйича дастлабки билимлар даражасини ташхис қилиш мақсадида қўлланилади.

Методни амалга ошириш тартиби:

- иштирокчилар машғулот қоидалари билан таништирилади;
- ўқувчиларга мавзуга ёки бобга тегишли бўлган сўзлар, тушунчалар номи туширилган тарқатмалар берилади (индивидуал ёки гуруҳли тартибда);
- ўқувчилар мазкур тушунчалар қандай маъно англатиши, қачон, қандай ҳолатларда қўлланилиши ҳақида ёзма маълумот берадилар;
- белгиланган вақт якунига етгач ўқитувчи берилган тушунчаларнинг тугри ва тулиқ изоҳини уқиб эшиттиради ёки слайд орқали намойиш этади;
- ҳар бир иштирокчи берилган тўгри жавоблар билан узининг шахсий муносабатини таққослайди, фарқларини аниқлайди ва ўз билим даражасини текшириб, баҳолайди.

Намуна: “Модулдаги таянч тушунчалар таҳлили”

Тушунчалар	**Сизнингча бу тушунча қандай маънони англатади?**	**Қўшимча маълумот**
Инцидент	Стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай инцидентга айтилади.	

Маълумот	Техника воситалари ёрдамида қидириш,қабул қилиш, сақлаш, ишлов бериш, узатиш мумкин бўлган шаклга келтирилган ҳар қандай информация.	
Инцидентни бошқариш	Бизнес жараёнларни олиб бориш жараёнида иш ҳолатини тезда минимал хавф билан нормал иш ҳолатига қайтариш фаолияти ҳисобланади, ҳамда қисқа давом этадиган ва бир мақсад сари йўналтирилган хизматлар қаторига киради.	
Ролларни тақсимлаш	Асосий ҳаракатлардан бири ҳисобланади, инцидентларни бошқариш жараёнларини қуриш тажрибасига асосан йўлларни танлаб, улар орасидан хато йўлларни ажратиш орқали амалга оширилади.	
Ишчи маълумотларни ошкор қилиш	Корхона ёки ушбу маълумот чиқиб кетмаслиги зарур бўлган ҳудуд доирасидан ахборотни чиқариш назарда тутилади.	
Ҳисоботларни сохталаштириш	Билиб туриб маълум бир ҳаракатлардан кейин маълумотларни нотўғри акс эттириш. Сохталаштириладиган ҳужжатлар корхонананинг ички ҳужжатлари ёки ташқи алоқалари ҳужжатлари бўлиши мумкин.	

Изоҳ: Иккинчи устунчага қатнашчилар томонидан фикр билдирилади. Мазкур тушунчалар ҳақида қўшимча маълумот глоссарийда келтирилган.

Венн Диаграммаси методи

Методнинг мақсади: Бу метод график тасвир орқали ўқитишни ташкил этиш шакли бўлиб, у иккита ўзаро кесишган айлана тасвири орқали ифодаланади. Мазкур метод турли тушунчалар, асослар, тасавурларнинг анализ ва синтезини икки аспект орқали кўриб чиқиш, уларнинг умумий ва фарқловчи жиҳатларини аниқлаш, таққослаш имконини беради.

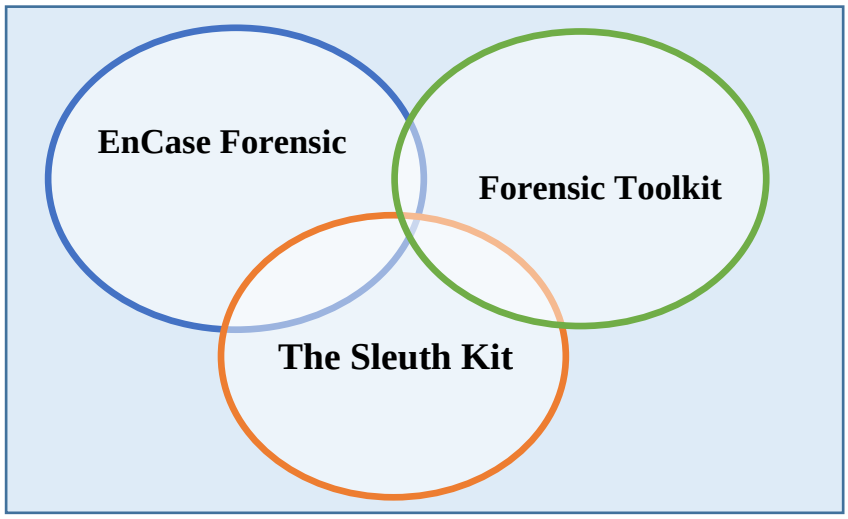
Методни амалга ошириш тартиби:

- иштирокчилар икки кишидан иборат жуфтликларга

бирлаштириладилар ва уларга кўриб чиқилаётган тушунча ёки асоснинг ўзига хос, фарқли жиҳатларини (ёки акси) доиралар ичига ёзиб чиқиш таклиф этилади;

- навбатдаги босқичда иштирокчилар тўрт кишидан иборат кичик гуруҳларга бирлаштирилади ва ҳар бир жуфтлик ўз таҳлили билан гуруҳ аъзоларини таништирадилар;
- жуфтликларнинг таҳлили эшитилгач, улар биргалашиб, кўриб чиқилаётган муаммо ёҳуд тушунчаларнинг умумий жиҳатларини (ёки фарқли) излаб топадилар, умумлаштирадилар ва доирачаларнинг кесишган қисмига ёзадилар.

Намуна: Криминалистик изланишлар



“Блиц-ўйин” методи

Методнинг мақсади: ўқувчиларда тезлик, ахборотлар тизмини таҳлил қилиш, режалаштириш, прогнозлаш кўникмаларини шакллантиришдан иборат. Мазкур методни баҳолаш ва мустаҳкамлаш максадида қўллаш самарали натижаларни беради.

Методни амалга ошириш босқичлари:

1. Дастлаб иштирокчиларга белгиланган мавзу юзасидан тайёрланган топшириқ, яъни тарқатма материалларни алоҳида-алоҳида берилади ва улардан материални синчиклаб ўрганиш талаб этилади. Шундан сўнг, иштирокчиларга тўғри жавоблар тарқатмадаги «якка баҳо» колонкасига белгилаш кераклиги тушунтирилади. Бу босқичда вазифа якка тартибда бажарилади.

2. Навбатдаги босқичда тренер-ўқитувчи иштирокчиларга уч кишидан иборат кичик гуруҳларга бирлаштиради ва гуруҳ аъзоларини ўз фикрлари билан гуруҳдошларини таништириб, баҳслашиб, бир-бирига таъсир ўтказиб, ўз фикрларига ишонтириш, келишган ҳолда бир тўхтамга келиб, жавобларини «гуруҳ баҳоси» бўлимига рақамлар билан белгилаб чиқишни топширади. Бу

вазифа учун 15 дақиқа вақт берилади.

3. Барча кичик гуруҳлар ўз ишларини тугатгач, тўғри ҳаракатлар кетма-кетлиги тренер-ўқитувчи томонидан ўқиб эшиттирилади, ва ўқувчилардан бу жавобларни «тўғри жавоб» бўлимига ёзиш сўралади.

4. «Тўғри жавоб» бўлимида берилган рақамлардан «якка баҳо» бўлимида берилган рақамлар таққосланиб, фарқ булса «0», мос келса «1» балл қуйиш сўралади. Шундан сўнг «якка хато» бўлимидаги фарқлар юқоридан пастга қараб қўшиб чиқилиб, умумий йиғинди ҳисобланади.

5. Худди шу тартибда «тўғри жавоб» ва «гуруҳ баҳоси» ўртасидаги фарқ чиқарилади ва баллар «гуруҳ хатоси» бўлимига ёзиб, юқоридан пастга қараб қўшилади ва умумий йиғинди келтириб чиқарилади.

6. Тренер-ўқитувчи якка ва гуруҳ хатоларини тўпланган умумий йиғинди бўйича алоҳида-алоҳида шарҳлаб беради.

7. Иштирокчиларга олган баҳоларига қараб, уларнинг мавзу бўйича ўзлаштириш даражалари аниқланади.

«Инцидентга жавоб қайтаришнинг асосий босқичлари» кетма-кетлигини жойлаштиринг. Ўзингизни текшириб кўринг!

Ҳаракатлар мазмуни	Якка баҳо	Якка хато	Тўғри жавоб	Гуруҳ баҳоси	Гуруҳ хатоси
Инцидент юзага келишига тайёр бўлиш.					
Инцидентларни ўрганиб чиқиш бўйича комиссия тузиш (CSIRT).					
Инцидентни аниқлаш - ахборот хафсизлиги инцидентини идентификацияси.					
Бошланғич жавоб қайтариш - биринчи даражали тергов ишларини бошланиши, асосий воқеаларни ёзиб олиш, комиссия тузилиш, тергов олиб борилишига алоқадор шахслар аниқланиш. Қонунга хилоф ҳаракатларни аниқлаш.					

“Брифинг” методи

“Брифинг”- (инг. briefing-қисқа) бирор-бир масала ёки саволнинг муҳокамасига бағишланган қисқа пресс-конференция.

Ўтказиш босқичлари:

1. Тақдимот қисми.
2. Муҳокама жараёни (савол-жавоблар асосида).

Брифинглардан тренинг якунларини таҳлил қилишда фойдаланиш мумкин. Шунингдек, амалий ўйинларнинг бир шакли сифатида қатнашчилар билан бирга долзарб мавзу ёки муаммо муҳокамасига бағишланган брифинглар ташкил этиш мумкин бўлади.Талабалар ёки тингловчилар томонидан яратилган мобил иловаларнинг тақдимотини ўтказишда ҳам фойдаланиш мумкин.

“Портфолио”методи

“Портфолио” – (итал. portfolio-портфель, инг.ҳужжатлар учун папка) таълимий ва касбий фаолият натижаларини аутентик баҳолашга хизмат қилувчи замонавий таълим технологияларидан ҳисобланади. Портфолио мутахассиснинг сараланган ўқув-методик ишлари, касбий ютуқлари йиғиндиси сифатида акс этади. Жумладан, талаба ёки тингловчиларнинг модул юзасидан ўзлаштириш натижасини электрон портфолиолар орқали текшириш мумкин бўлади. Олий таълим муассасаларида портфолионинг қуйидаги турлари мавжуд:

Фаолият тури	**Иш шакли**	
	Индивидуал	**Гуруҳий**
Таълимий фаолият	Талабалар портфолиоси, битирувчи, докторант, тингловчи портфолиоси ва бошқ.	Талабалар гуруҳи, тингловчилар гуруҳи портфолиоси ва бошқ.
Педагогик фаолият	Ўқитувчи портфолиоси, раҳбар ходим портфолиоси	Кафедра, факультет, марказ, ОТМ портфолиоси ва бошқ.

III. НАЗАРИЙ МАШҒУЛОТЛАР МАТЕРИАЛЛАРИ

1-маъруза.
Мавзу: Ахборот хавфсизлиги инцидентларини бошқаришда норматив базалар

Режа:

Кириш.

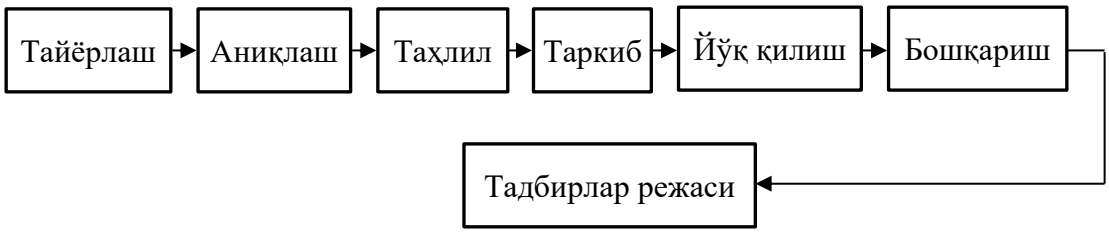
1. Ахборот хавфсизлиги инцидентларини бошқариш бўйича методология.
2. Ахборот хавфсизлиги инцидентларини бошқаришда ISO/IEC 27035:2016 стандартининг ўрни.
3. Ахборот хавфсизлиги инцидентларини бошқаришда ISO/IEC 27037 стандартининг ўрни.

Кириш

Ахборот хавфсизлиги инциденти – бу ахборот хавфсизлиги тизимидаги бир ёки бир неча тасодифий ва кутилмаган ҳодисалар, иш жараёнларини таҳлил қилишга катта имконият бериш ва ахборот ҳимоясини таҳдидга қўйилишидир.

Ахборот хавфсизлиги инциденти – бу ахборот хавфсизлиги тизимига амалга ошириладиган ҳодисалар, ахборот хавфсизлигига кутилган ва кутилмаган таҳдидлар йиғиндисидир.

Ахборот хавфсизлиги инцидентларини бошқариш бўйича методология



1.1-расм. Ахборот хавфсизлиги инцидентини бошқаришнинг хаёт даври

1. Action Plan (Тадбирлар режаси) – бу инцидентларга қарши чора-тадбирларни умумий режаси.
2. Prepare (Тайёрлаш) - бу маълумотларни сақлаш ва инцидентга жавоб қобилиятини такомиллаштириш (режалаштириш ва тайёрлаш).
3. Detect (Аниқлаш) - бу маълумотларни саралаш ва ўрганиш жараёнида инсидентларни аниқлаш.
4. Analyze (Таҳлил қилиш) – бу жараён ва маълумотларни назорат қилиш, таҳлил қилиш, кузатиш ва қайта тиклаш.

5. Contain (Сақлаш) - бу зарарларни камайтириш, ахборотни ўғирлашдан ҳимоялаш, хизмат кўрсатишдаги ўз улушларини назоратлаш.

6. Eradicate (Барҳам бериш) – бу тизимга нисбатан таҳдидларни бартараф этиш.

7. Recover (Қайта тиклаш) – бу хавфсиз ва тезкорлик билан ҳисоблаш тизимларини қайта тиклаш ва ҳ.к.з.

8. Manage (Бошқариш) – бу инсидентларни бошқариш жараёни.

Ахборот хавфсизлиги инцидентларини бошқаришда ISO/IEC 27035:2016 стандартининг ўрни

ISO/IEC 27035-1:2016 Ахборот технологиялари. Хавфсизлигни таъминлаш усуллари. Ахборот хавфсизлиги тизимидаги тасодифларни бошқариш - 1-Қисм: Инцидентни бошқариш принциплари.

ISO/IEC 27035-2:2016

Ахборот технологиялари. Хавфсизлигни таъминлаш усуллари. Ахборот хавфсизлиги тизимидаги тасодифларни бошқариш - 2-Қисм: Инсидентга жавоб қайтаришни режалаштириш ва тайёрлаш бўйича қўлланма.

ISO/IEC 27035-1:2016, 1-Қисм: Инцидентни бошқариш принциплари.

ISO/IEC 27035 стандартнинг ушбу қисми бир неча қисмлардан ташкил топган бутун халқаро стандарт учун асос бо`либ ҳисобланади. Унда АХ инсидентлари тушунишда ва бошқаришда асосий тушунчаларни аниқлаштириб,уларнинг аниқланишида структурали ёндашув принсипларини, ахборотлаштиришни, баҳолашни, ўз вақтида реакция кўрсатишни ҳамда тажрибаларда хулоса чиқариш тушунчаларини қамраб олган. Стандартда келтирилган принциплар умумий ҳисобланиб, ташкилотларнинг тури, ҳажми ва характеридан қатъий назар фойдаланишлари мумкин. Ташкилотлар ўзларининг тури, ҳажми ва характеридан келиб чиққан ҳолда АХ инцидентлари хавф ҳатарларига қарши чораларни стандартда келтирилган кўрсатмалар асосида мослаштиришлари мумкин. Бу стандарт АХ инцидентлари менежменти хизматини кўрсатувчи ташқи ташкилотлар томонидан ҳам ишлатилиши мумкин.

ISO / IEC 27035-1: 2016 кўп қисмли халқаро стандарт ҳисобланади. Бу стандартда ахборот хавфсизлиги инцидентларини бошқаришни этаплари ва асосий тушучалари, инцидентларга жавоб қайтариш ва баҳолашлари кўрсатиб ўтилган.

ISO / IEC 27035-1: 2016 стандартида келтирилган принциплар корхонанинг характери ва ҳажмига қарамасдан туриб ҳам бемалол қўлланишга мўлжалланган.

Корхоналар ISO / IEC 27035-1: 2016 стандартида келтирилган

тавсияларни ахборот хавфсизлиги хавф-хатарларини турига, ҳажмига ва характерига қараб тўғрилашлари мумкин.

Бу стандарт бундан ташқари ахборот хавфсизлиги инцидентларини бошқариш хизматларини кўрсатиб берувчи ташқи корхоналарда ҳам қўлланилади.

Ҳужжат структураси қуйидагича:

Муқаддима.

0. Кириш.

1. Қўлланилиш соҳаси.

2. Норматив ссилкалар.

3 Атама ва терминлар.

4. Маълумот.

5. Босқичлар.

А Илова (маълумотнома): АХ инцидентларига мисоллар ва уларнинг сабаблари;

В Илова (маълумотнома): Тергов ишлари ва стандартларнинг ўзаро алоқаси;

С Илова (маълумотнома): ISO/IEC 27001 ва ISO/IEC 27035 стандартлар орасидаги кесишув ссилкалари жадвали.

ISO/IEC 27035-2:2016, 2-Қисм: Инцидентга жавоб қайтаришни режалаштириш ва тайёрлаш бўйича қўлланма.

ISO/IEC 27035-2 стандарти АХ инцидентларига реаксия қилиш бўйича кўрсатмаларни ўз ичига олади. ISO/IEC 27035-2 стандартига кўра кўрсатмалар “Режалаштириш ва тайёрланиш”, “Хулоса чиқариш” этапларига ва “АХ инцидентлари бошқариш этаплари” моделига асосланган.

Стандартда келтирилган принциплар умумий ҳисобланиб, ташкилотларнинг тури, ҳажми ва характеридан қатъий назар фойдаланишлари мумкин. Ташкилотлар ўзларининг тури, ҳажми ва характеридан келиб чиққан ҳолда АХ инцидентлари хавф қатарларига қарши чораларни стандартда келтирилган кўрсатмалар асосида мослаштиришлари мумкин. Бу стандарт АХ инцидентларини бошқариш хизматини кўрсатувчи ташқи ташкилотлар томонидан ҳам ишлатилиши мумкин.

Ҳужжат структураси қуйидагича:

Муқаддима.

0. Кириш.

1. Қўлланилиш сохаси.

2. Норматив ссилкалар.

3. Терминлар, атамалар ва қисқартмалар.

4. Ахборот хавфсизлиги инцидентларини бошқариш сиёсати.

5. АХ сиёсатининг янгиланиши.

6. АХ инцидентларини бошқариш бўйича режалар яратиш.

7. Инцидентларга жавоб қайтарувчи гуруҳларни шакллантириш (Incident Response Team, IRT).

8. Бошқа ташкилотлар билан муносабатларни яхшилаш.

9. Техник ва бошқа қўллаб-қувватловлар билан таъминлаш.

11. АХ инцидентларини бошқариш бўйича режаларни тестлаш.

12. Тажрибадан хулоса чиқариш.

Ахборот хавфсизлиги инцидентларини бошқаришда ISO/IEC 27037 стандартининг ўрни

ISO/IEC 27037-2014

Информацион технологиялар. Хавфсизликни таъминловчи метод ва воситалар.

Бу стандар рақамли ҳолда келтирилган потенциал далиллар билан муомила қилиш жараёнларига оид аниқ йўл-йўриқларни намойиш этади. Бу жараёнларга қуйидагилар киради: идентификация, рақамли ҳолда келтирилган потенциал далилларни йиғиш, олиш ва сақлаш. Бу жараёнлар рақамли ҳолда келтирилган далилларнинг бутунлигини таъминлашда ҳамда тергов қилиш учун керак бўлади. Бу стандарт рақамли ҳолда келтирилмаган далиллар учун ҳам умумий ёриқномаларни ўз ичига олади. Булар эса ўз ўрнида рақамли ҳолда келтирилган потенциал далилларни таҳлил қилиш пайтида фойдали бўлиши мумкин.

Ушбу стандарт рақамли кўринишда бўлган далилларнинг ишончлилигини аниқловчи шахсларни ахборотлаш учун ҳам мўлжалланган. Бу стандарт рақамли кўринишда бўлган потенциал далилларнинг намойиш қилинишига, таҳлилга ва ҳимояга муҳтож ташкилотларда қўлланилиши мумкин. Бу стандарт рақамли кўринишда бўлган дадиллар (кўп ҳолларда катта ва мураккаб дадиллар) билан боғлиқ бўлган, жараёнлари ҳосил қилувчи ва уларни баҳолайдиган бошқарув органлари учун муҳим ҳисобланади.

Ҳақиқий стандартда кўрсатиб ўтилган потенциал далиллар рақамли қурилмалар, тармоқлар, маълумотлар базаси ва бошқа турли рақамли воситалардан олинган бўлиши мумкин. Чунки бу далиллар ҳосил бўлишида йўқ рақамли форматга эга ҳисобланади. Ҳақиқий стандарт аналогли маълумотларни рақамли маълумотларга ўзгартириш муаммосини қамраб олмаган.

Қўлланилиш соҳаси

Ҳақиқий стандарт ўзида қийматга эга, рақамли кўринишда бўлган далиллар(буларга идентификация, рақамли ҳолда келтирилган потенциал далилларни йиғиш, олиш ва сақлаш киради) билан муомила қиладиган аниқ

соҳалар тўгрисида юриқномаларни қамраб олган. Ҳақиқий стандарт рақамли кўринишдаги далиллар билан ишлаш жараёнида келиб чиқадиган кенг тарқалган ҳолатлар бўйича кўрсатмаларга эга. Ҳақиқий стандарт ташкилотларда рақамли коринишда бўлган потенсиал далилларнинг юрисдикциялар орасида алмашинув жараёнини енгиллаштириб, интизомий жараёнларни амалга оширишга ҳизмат қилади.

Ҳақиқий стандарт ўзида турли хил холатларда ишлатиладиган қуйидаги қурилмалар ва функциялар ҳақида тавсиялар беради:

турли компютерларда ишлатиладиган рақамли маълумот ташувчилар, масалан, қаттиқ диск, дискеталар, оптик ва магнитли дисклар;

Мобил телефонлар, “Чўнтак” шахсий компютерлар, шахсий электрон қурилмалар, хотира карталари;

– мобил навигацион тизимлар;

– рақамли фотоаппаратлар ва видеокамералар;

– тармоқга уланадиган турли компютерлар;

– TCP/IP протоколига асосланган тармоқлар ва бошқа рақамли протоколлар;

– юқорида санаб ўтилган қурилмалар функциясига асосланган қурилмалар.

Фойдаланилган адабиётлар

1. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. М60 Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 170 с.
2. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари.
3. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари.
4. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.
5. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
6. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

2-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларини бошқариш тизими

Режа:

1. Ҳодисалар ва ахборот хавфсизлиги инцидентлари тушунчаси.
2. Бошқариш функцияси ва моҳияти.
3. Бошқариш турлари, принциплари ва ёндашувлари.
4. Ахборот хавфсизлиги инцидентларини мақсади ва вазифалари.

Ҳодисалар ва ахборот хавфсизлиги инцидентлари тушунчаси

Инцидент (можоро, ҳодиса) - бу стандарт бўлиши мумкин бўлмаган ҳодисалар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади. Ахборот хавфсизлиги инциденти – бу ахборот хавфсизлиги тизимига амалга ошириладиган ҳодисалар, ахборот хавфсизлигига кутилган ва кутилмаган таҳдидлар йиғиндисидир.

Ахборот хавфсизлиги инцидентлари билан ишлаш

Бунда гап инцидентлар хавфсизлиги хақида боради. Ахборот хавфсизлиги режими ўрнатилгандан (хужжатлар қабул қилинган, техник қисмлари ўрнатилган ва созланган бўлиб, биринчи тренинглар ўтқазилган) сўнг энг кўп вақт инцидентлар билан ишлашга кетади.

Инцедентлар ҳакида маълумот бериш

Биринчи бўлиб инцедент хақида маълумот олиш лозим. Бу хақда хавфсизлик сиёсатини ишлаб чиқиш ва ходимлар учун ахборот хавфсизлиги инцедентлари бўйича амалий қўлланмани тайёрлашни ўйлаб кўриш лозим.

Ахборотнинг асосий манбалари:

1. Helpdesk.

Қурилма ишидаги ҳар қандай муаммолар вужудга келганда сизнинг IT-хизмат хелпдеск га ёзишади ёки қўнғироқ килишади. Шунинг учун олдиндан бизнес-жараёнга хэлпдеск ни “бириктириб” қўйиш ва АХ бўлимига юбориладиган инцендентлар турини кўрсатиш лозим.

2. Фойдаланувчилардан келган тўғридан-тўғри хабарлар.

Ягона контакт марказини ташкил этиб, бу хақда АХ тренингда ходимларга этиш лозим. Ҳозирги кунда ташкилотлардаги АХ бўлимлари унчалик каатта эмас, шунинг учун инцидентларни қабул қилишга маъсул ходим тайинлаш қийин бўлмайди.

3. АХ ходимлари томонидан аниқланган инцидентлар.

Бунда хаммаси оддий ва бу каби қабул каналини ташкил этишда жисмоний харакат талаб этилмайди.

4. Журналлар ва огохлантириш тизимлари.

Антивирус консоли, IDS, DLP ва бошқа хавфсизлик тизимларида огохлантиришни созланг. Ташкилотга ўрнатилган аггрегаторлардан фойдаланиш қулайроқ хисобланади. Аггрегаторлар тизим ва дастур логларидан маълумотлар йиғади. Ташқи тармоққа уланган жойларга алохида эътибор бериш лозим.

Бошқариш функцияси ва моҳияти

Хозирги пайтда халқаро амалиётда АХ инцидентларни бошқаришга оид етарлича норматив хужжатлар ишлаб чиқилган. Инцидентларни бошқариш саволлари нафақат АХ доирасида балки бутун ИТ-сервис келиб чиқади. ISO 20000:2005 халқаро стандартларнинг Service Delivery and Support бўлимида ИТ-инфраструктурада инйидентларни бошқаришни ташкиллаштиришга оид бир қанча талаблар келтирилган. Ушбу стандартга кўра инцидент деб “хизмат функционаллигининг нормал элементи хисобланмайдиган ва бу билан хизмат сифатини пасайишига олиб келадиган ҳар қандай ҳодиса” тушунилади.

АХ даги инцидент бошқарувига оид хусусий саволлар қуйидаги хужжатларда кўриб чиқилади:

ISO/IEC 27001:2005 Information security management system. Requirements. Ушбу стандарт доирасида АХ бошқариш тизимини қуришга умумий талаблар келтирилган.

ISO/IEC TR 18044 Information security incident management. Ушбу хужжат (plan–do–check–act or plan–do–check–adjust) PDCA циклик модели доирасида инцидентларни бошкариш инфраструктурасини тавсифлайди.

Режалаштириш, эксплуатация ва жараённи анализ килиш хақида батафсил йўриқномалар келтирилган.

CMU/SEI-2004-TR-015 Defining incident management processes for CISRT. Бу хужжат инцидентларни бошқариш жараёнини яхшилаш, сингдириш ва режалаштириш методологиясини тавсифлайди. Асосий пойдевор CISRT (Critical Incident Stress Response Team) организатсия ишининг асосий пойдевори – ахборот хавфсизлиги инцидентларига ўз вақтида реакция қилиш, қайта ишлаш , олдини олишга кўмаклашиш ва сервис хизматларни таминловчи бўлим ёки гурух.

Ушбу тахлиллар жараёнида барча тавсияларни кўриб чиқишнинг имконияти бўлмаганлиги сабабли , ташкилотлар учун алохида методолигаялар мос равишда ишлаб чиқилгани эффективроқ хисобланади. Лекин ишлаб чиқилган методология замонавий бошқариш тизими стандартларига зид келмаслиги лозим. Бу замонавий бошқариш тизими стандартларига мисол қилиб ISO/IEC 27001 и ISO 20000 олиш мумкин.

Бошқариш турлари, принциплари ва ёндашувлари

ISO/IEC 27001 халқаро стандарти "Ахборот технологиялари - Хавфсизлик методлари - Ахборот хавфсизлиги бошқаруви тизимлари - Талаблар" қуйидагиларга таъриф беради:

- АХ ҳодисалари: тизим ёки тармоқ холати хақидаги аниқланган ҳодиса бўлиб, АХ сиёсатини бузилган бўлиши мумкинлиги ёки хавфсизликка оид илгари дуч келмаган нотаниш холатидир;
- АХ инциденти: олдиндан кўрилмаган ва бизнес-ахборотни йўколишига ва АХ га таҳдид келтириб чикариши мумкин бўлган АХ ҳодисасидир.

Ушбу маълумотлар доирасида мавжуд ҳамма инцидент бошқарувига оид тавсияларни кўриб чиқиб бўлмайди ва маълум бир ташкилот учун бошқа методология ишлатиш мақсадга мувофиқ бшлиши мумкин. Лекин ҳар кандай методология асосий замонавий стандартлар, масалан ISO/IEC 27001 ва ISO 20000 билан мос тушиши керак. Батафсил: http://www.jetinfo.ru/stati/upravlenie-intsidentami

A.13 Ахборот хавфсизлиги инцидентларини бошқариш

A.13.1.1 Ахборот хавфсизлиги ҳодисалари ҳақидаги хабар. Ушбу хабар маълум мўлжалланган бошқарув каналлари орқали иложи борича тез юборилиши керак

A.13.1.2 Хавфсизликнинг заифликлари ҳақидаги хабар. Барча информацион тизимга таалуқли бўлган ходимларни, ишчиларни ва бошқа ходимларни кузатилаётган заифликларни кузатиб бориб улар ҳақида хабар беришларини таъминлаш

A.13.2.1 Жараёнлар ва жавобгарлик. Бунда бошқармаларга жавобгарлик юкланиши керак бўлиб , ахборот хавфсизлиги инцидентларига қарши тўғри, эффектив ва тезкор чора кўриш жараёнини таминлашни аниқлаштириш.

A.13.2.2 Ахборот хавфсизлиги инцидентларидан хулоса чиқариш. Бунда ахборот хавфсизлиги инцидентларининг хажми ўлчаш, унинг типини аниқлаш ва қийматини аниқловчи механизмларни амалга ошириш тушунилади.

A.13.2.3 Далилларни йиғиш. Ахборот хавфсизлиги инциденти сифатида бирор бир шахс ёки ташкилотлар қараладиган бўлса ҳуқуқни мухофаза қилиш органларига далилларни йиғиш , сақлаш ва тақдим этиш лозим бўлади.

АХ инцидентларини бошқариш этаплари

Режалаштириш ва таёргарлик кўриш:

– АХ инцидент менежменти сиёсати ва бош рахбариятнинг ундаги мажбуриятлари;

– АХ инцидентини бошқариш тизими;

– корпоратив хавфсизлик ва хавфсизлик тизими, таҳлил ва хавф-хатарларни бошқариш, АХ сиёсатини янгилаш;

– АХ инцидентлари ҳақида кўрсатмалар бериш ва ўргатиш;

– АХ инцидент менежменти тизимини тестлаш.

Қўлланилиши:

– АХ ҳодисаларини аниқлаш ва улар ҳақида хабар бериш;

– баҳолаш ва хулоса чиқариш: Ушбу ҳодиса инцидентми ёки ёқ;

– АХ инцидентига қонуний экспертиза асосида реакция қилиш.

Таҳлил:

– қўшимча қонуний экспертиза;

– йиғилган тажрибани умумлаштириш;

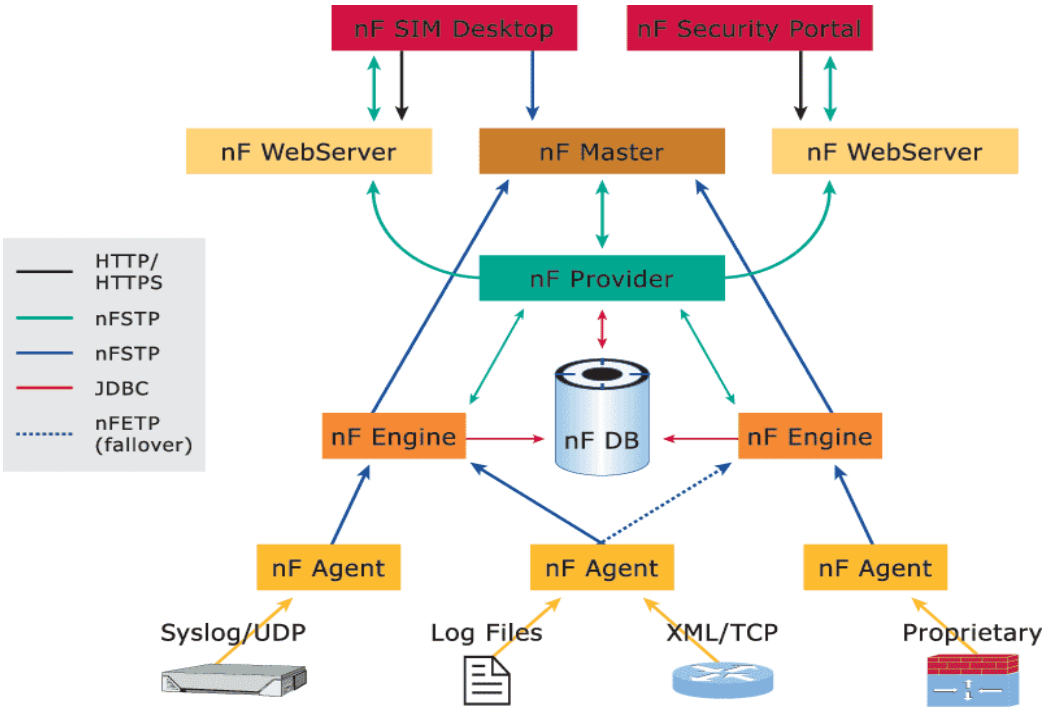
– хавфсизликни яхшилаш методларини аниқлаш;

– АХ инцидентларини бошқариш тизимини яхшилаш усулларини аниқлаш.

Яхшилаш:

– менежмент анализи ва хавфсизлик риски анализи натижаларини қайта аниқлаштириш;

– АХ инцидентларини бошқариш тизимини яхшилаш чораларни ўтказиш.



2.1-расм. NetForensics дастури узлуксиз равишда хавфсизлик ҳодисаларини кўрсатиб беради, кайта ишлайди ва йиғади

NetForensics ахборот хавфсизлигини бошқариш тизими ахборот хавсизлигини гетероген мухитида таминлаш воситалари билан ишлаш учун мўлжалланган. У узлуксиз равишда хавфсзлик ҳодисаларини кўрсатиб беради, кайта ишлайди ва йиғади.

Ахборот хавфсизлиги инцидентларини бошқаришнинг мақсади ва вазифалари

Инцидентларни бошқаришни эффектив равишда ташкил етиш ва амалий

кўллаш корхонага қуйидаги бизнес устунликларни беради:

- Бизнес ташкилотларга инцидентларнинг салбий таъсирини камайтириш.
- Ахборот хавфсизлигини яхшилаш бўйича чораларни аниқлаш.

Ахборот хавфсизлиги бўлинмаларида инцидентларни бошқариш жараёнини тўғри ташкил етилиши бу:

- Барча мутаххасисларга ролларни ва инцидентларга ўз вақтида ва сифатли реакция қилишни аниқ тақсимлаш;
- Химоя чоралари эффективлиги мониторингига тезкор ахборот;
- Бўлинмалардаги ходимларнинг ишлаш самарадорлигини назоратлашнинг шаффофлиги; бизнес-бўлинмалари ва ахборот технологияларга тегишли ходимларнинг ўзаро ҳамкорлиги сифатини ошириш.

Инцидентларни бошкариш жараёнини автоматлаштириш тизими куйидагиларни имконини беради:

- АХ ҳақидаги инцидентлари ва ходисаларини саклаш ва кайта ишлаш;
- рўй берган инцидентларни, олдинроқ рўй берган инцидентлар анализига асосланиб бартараф етиш; йиғилган маълумотларни таҳлил қилиш.

Фойдаланилган адабиётлар

1. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. М60 Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 170 с.
2. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари.
3. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари.
4. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

5. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

6. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

3-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларини бошқариш сиёсати. Ахборот хавфсизлиги инцидентларини бошқариш жараёни

Режа:

1. Ахборот хавфсизлиги инцидентларини бошқаришда ташкилот ва муассасаларда инцидентларга қарши курашиш сиёсатини ишлаб чиқиш.
2. Ахборот хавфсизлиги инцидентлари структураси. Тезкор жавоб қайтариш.
3. Ахборот хавфсизлиги инцидентларининг классификацияси.

Ахборот хавфсизлиги инцидентларини бошқаришда ташкилот ва муассасаларда инцидентларга қарши курашиш сиёсатини ишлаб чиқиш

Ахборот хавфсизлиги инцидентлари бошқариш сиёсатини (АХИБС) шакллантириш муаммоларини ечишда муҳим вазифа АХИ бошқариш муолажаси детализацияси ва АХ инцидентлари бошқаруви формаллашган моделини қуриш билан боғлиқ. АХИ бошқарув муолажасини изоҳлаш учун PCDA модели – жараёнларни узлуксиз яхшилаш классик моделидан фойдаланилади. АХИБС ни формал намойиши учун қуйидаги вазифа ечимларини кўриб чиқувчи комплекс ёндашув танланган:

- Ахборот хавфсизлиги инцидентлари ҳисоблаш, маълум қилиш ва аниқлаш.
- Ахборот хавфсизлиги инцидентларига реакция, олдини олиш учун керакли воситалар қўлланилиши ва етказилган зарарни тиклаш ва камайтириш.
- Ахборот хавфсизлигини бутунлигича таъминлаш жараёнини яхшилаш ва олдини олувчи ҳимоя чораларини режалаштириш мақсадида содир бўлган инцидентларни таҳлиллаш.

Формаллашган модел назарий-кўплик ва мантқий шаклларда намойиш этилади. Таклиф этилаётган АХИБС формаллашган модели компанияга

етказиладиган зарар ҳақида огоҳлантирмайди, бироқ уни ташкил этиш орқали ташкилотнинг мавжуд ҳимоя тизимини самарадорлигини ошириш ва қайта зарар кўриш эҳтимолини камайтиришга эришиш мумкин.

Ахборот хозирги кунда ташкилотнинг рақобатбардошлигини таъминловчи асосий ресурслардан бири бўлиб, ташкилот ҳимоя масаларини ҳам актуаллаштиради. Ахборотни ҳимоялаш тизимидаги заифликлар молиявий йўқотишларга, тижорий операцияларга зарар етказишга ва натижада компанияни “бозор учун кураш”дан чиқариб юборилишига олиб келиши мумкин. Шундай экан замонавий компанияларнинг биринчи стратегик вазифаси тизимда содир бўлувчи ахборот хавфсизлиги инцидентларини бошкариш имконияти мавжуд ахборотни самарали ҳимоялаш тизимини яратиш ҳисобланади.

ГОСТ Р 18044-2007 “Ахборот технологиялари. Хавфсизликни таъминлаш воситалари ва методлари”га асосан, “ахборот хавфсизлиги инциденти - АХ таҳдид яратилиши ва бизнес-операциялар ўзаро келишиш эҳтимолий қиймати билан боғлиқ бир ёки бир неча кутилмаган АХ ҳодисаларини пайдо бўлишидир”.

Уларнинг натижаси ахборотни фош этилиши ёки ўзгартирилиши, ўчирилиши ёки ахборотни фойдаланмайдиган қилиб қўйувчи бошқа ҳодисалар ва ташкилот активларига зарар етказилиши ёки ўғирланиши бўлиши мумкин.

Инцидент сифатида аниқланган, лекин бу ҳақда хабар қилинмаган АХ инцидентларини ўрганиб чиқиш мумкин эмас ва бу инцидентларини олдини олиш учун ҳимоя чораларини кўришнинг иложи йўқ.

Бунга қарамасдан ташкилотда АХИ содир бўлганлик эҳтимоли уч асосий факторга мос бўлиши керак:

- АХИ ҳақидаги хабар бир вақтнинг ўзида бир нечта манбалардан келади (фойдаланувчилар, IDS, журнал файллари);
- IDS кўплаб қайтарилувчи ҳодисалар ҳақида сигнал беради;
- Автоматлаштирилган тизимлар журнал файллар таҳлили инцидент

ҳодисаси бўлиш имконияти ҳақида тизим администратори хулосаси учун асос бўлади.

ГОСТ Р 53114-2008 “Ахборот ҳимояси. Ташкилотда ахборот хавфсизлигини таъминлаш. Асосий термин ва атамалар”га асосан ташкилотнинг ахборот хавфсизлиги бошқаруви “қўлланма бўйича координацияланган ҳаракат ва ташкилотнинг ички ва ташқи муҳит ўзгарувчи шартларига мос АХ ни ташкилотда таъминлашни бошқаришдир”. Жорий ГОСТга асосан ташкилот ахборот хавфсизлигини бошқариш сиёсати бизнес, ташкилот, унинг активлари ва технологиялари характеристикасига асосида аниқланиши керак:

- АХ соҳасидаги ҳаракатлар асосий принципи ва йўналиши, мақсадларини ўз ичига олувчи коцепциядан иборат;
- Хавфсизликни таъминлаш бўйича шартли мажбуриятларни, маъмурий-ҳуқуқий талабларни ҳамда бизнес талабларни эътиборга олади;
- АХ бошқарувига амал қилувчи ва бу бўйича ишлаб чиқилувчи ташкилот бошқарув таҳдидлари стратегиясига риоя этади;
- Таҳдидларни баҳолаш критерияларини ўрнатади;
- Ташкилот раҳбарияти тасдиқлайди.

Ташкилотда АХ бошқариш тизими ташкилот жорий ривожланиш умумий шартларини шакллантирувчи асосий факторлар, компания фаолияти характерини ҳисобга олган ҳолда амалга оширилувчи, ички ва ташқи хавфларни олдини олишга йўналтирилган, аниқ бир ташкилотда ахборот хавфсизлик инцидентларини бошқариш сиёсати каби аниқланувчи ташкилот АХИ бошқарув сиёсати шаклида намойиш этилади.

Бунда АХИБС ни самарали амалга ошириш учун ташкилот мониторинги, қўллаш ва узлуксиз ҳужжатлаштириш тизимини эксплутация қилиш ва функционал планда таъминланиши, тадбиқ қилиниши, ишлаб чиқилиши керак.

Натижали АХИБС га эришиш учун керакли режалаштиришдан сўнг кўрилган муолажа сиёсатларни, қатор тайёрланган ҳаракатларни ва

қуйидагиларни ўз ичига олувчи ҳаракатларни бажариш керак:

1. АХ инциденти бошқариш сиёсатини ишлаб чиқиш ва шакллантириш, яна юқори рахбариятдан бу сиёсат тасдиғини олиш;

2. АХ инцидентлар бошқариш тизимини батафсил ҳужжатлаштириш ва ишлаб чиқиш. ГОСТ Р 18044-2007 «Ахборот технологиялари. Хавфсизликни таъминлаш воситалари ва методлари. Ахборот хавфсизлиги инцидентлари бошқаруви»га биноан, АХ инцидентлари бошқариш тизимларини ҳужжатлаштириш АХ инцидентлар классификацияси учун жиддийлик шкаласи ва ҳужжатлаштирилган муолажалари ва маълумотлар фойдаланиш муолажаларга ҳаволалар билан боғлиқ ҳаракатларга мос ва бизнесни узлуксизлигини таъминлаш плани, тармоқ захираланиши ва сервислар тизими АХ инцидентлари ва ҳодисалари ҳақидаги ҳисоботлар шаклларидан иборат бўлиши керак;

3. кириш, чиқиш ёки ҳужум қилинаётган тизимда, сервисда ва (ёки) маълумотлар тармоғида жойлашган оқим мониторинги тадбиқ қилиш;

4. Иккиланувчи муолажани активлаштириш элементлари ва тармоқ ва (ёки) сервис, тизим хавфсизлик сиёсатига биноан бизнес узлуксиз режалаштириши бўйича ҳаракатлар;

5. Мониторингни олиб бориш ва ташкилот ички тартибли тафтиши ёки суд ишлари учун эҳтиёж бўлган ҳолатларда далилларни электрон шаклда ҳимояланган ҳолда сақлашни ташкил этиш;

6. АХ инцидентлари ҳақида тафсилотларни ташкилот ходимларига ва бошқа шахсларга ёки ташкилотларга юбориш;

7. АХ инцидентлари бошқариш тизимини, унинг жараёнларини ва муолажаларини синовдан ўтқазиш;

8. Бошқарув сиёсатини янгилаш ва АХ таҳдидлар таҳлили, АХ корпоратив сиёсатлари, тизим, сервислар учун ва (ёки) АХ инцидентлар бошқарувида ҳаволалар ишлаши учун тармоқлар АХ махсус сиёсати ва АХ инцидентлар бошқаруви тизими чиқиш маълумотлари контексида бу сиёсатларни давомий кўриб чиқишни таъминлаш;

9. АХ инцидентига қарши ҳаракат гуруҳи (АХИҚҲГ) персоналига мос дастурий билим ўргатиш;

10. АХ инцидент бошқариш тизимини (ва АХИҚҲГ фаолиятини) техник ва бошқа воситалар билан қўллаб-қувватлаш;

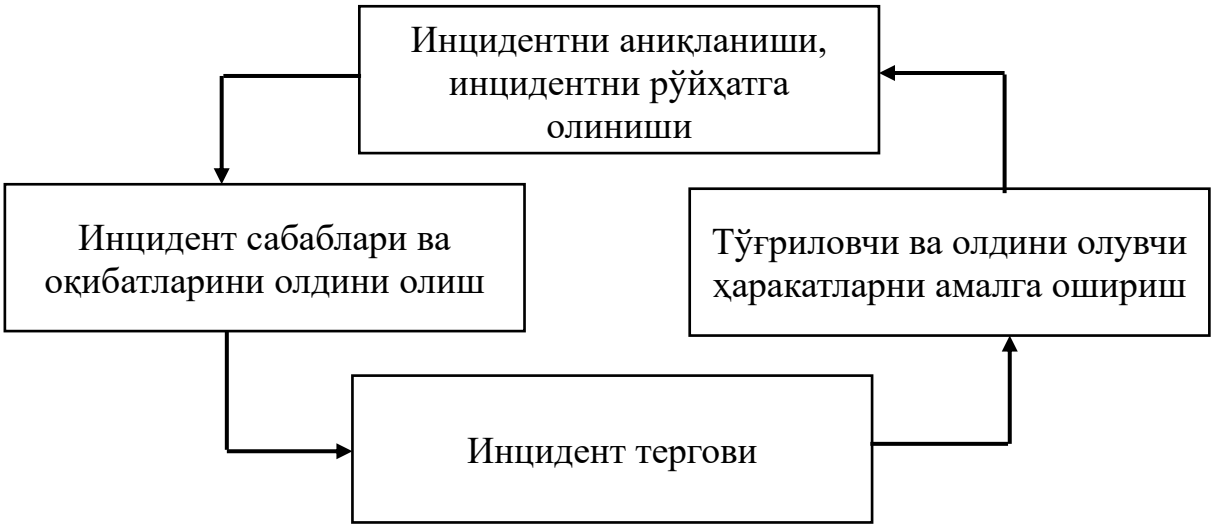
11. АХ инцидентларини бошқариш ҳақида хабардорликни таъминлаш дастурларини лойиҳалаш ва ишлаб чиқиш, ташкилотнинг барча персоналини бу дастур билан таништириш.

Ахборот хавфсизлиги инцидентлари структураси. Тезкор жавоб қайтариш

ГОСТ Р ИСО/МЭК 27001-2006 «Ахборот технологиялари. Хавфсизликни таъминлаш воситалари ва методлари. Ахборот хавфсизлиги бошқариш тизимлари. Талаблар»га асосан хусусий сиёсат ахборот хавфсизлиги ҳолати мониторингиумумий бошқариш принципларини ўрнатиши ва ташкилот АХ инцидентлари бошқарувини амалга ошириш учун натижалардан фойдаланиши керак. Бу ташкилотнинг барча технологик жараёнларига тадбиқ этилиши керак ва ташкилот барча ходимлари томонидан бажарилиши учун мажбурийдир. Жорий хусусий сиёсат талабларини амалга оширувчи ва бажарувчи ташкилотнинг АХ ни таъминлаш бўйича тадбирлар ташкилот тартиб-қоидаларига биноан ички норматив ҳужжатларида тасдиқланади.

Хавфсизлик инцидентларига қарши чоралар ва бошқариш изоҳларни талаб этади:

- хавфсизлик билан боғлиқ инцидентлар қайта ишловида ҳар бир ташкилотнинг роли ва фаолияти;
- хавфсизлик соҳасида инцидентлар белгиларини таниб олиниши ва кузатилиш муолажалари;
- хавфсизлик инцидентлари қайта ишлови муолажалари ва қарши ҳаракат усуллари;
- хавфсизлик соҳасидаги инцидентлар қайта ишловидан кейинги чораларни қабул қилиш.



3.1-расм. Ахборот хавфсизлиги инцидентлари бошқаруви муолажалари

Таҳдид ва инцидентларга қарши ҳаракатлар ва уни олдини олиш.

Ахборот хавфсизлиги бузилиш ва хавфларга самарали қарши ҳаракатлар миллий ахборот ташкилотлари, жавобгар органлар ва ҳуқуқий институтлар, ҳамда хавфсизлик авариялари инспексия ўтказувчи ва зарани баҳоловчи ташкилотлар орасида ҳамкорлик қилишни талаб этади. Бундан ташқари техник заифликларни таҳлилловчи ва техник қарши чораларни белгиловчи ташкилотлар билан ҳамкорлик ўрнатиш жуда муҳимдир.

Ахборот хавфсизлиги инцидентларини олдини олиш.

Ахборот хавфсизлигида авария ва бузилишларни олдини олиш мониторинг, ўрганиш ва ўзгаришларни бошқаришдан иборат. Миллий (компютер инцидентларига қарчи ҳаракат хизмати) CSIRT мониторинг бўйича асосий ташкилот ҳисобланади. Критик ҳудуд ахборот сиёсати билан мавжуд маълумот мониторинги мослигини таъминлашни тақазо этади. Шундай қилиб, ахборот сиёсати мониторингини масштабини муҳокама қилиш зарур. Бундан ташқари хусусий ва давлат ташкилоти ходимларини, яна кенг оммани ахборот хавфсизлиги таъминлаш бўйича сиёсат билан хабардор қилиш муҳим. Хавфсизлик масалалари бўйича ахборотга таъсир ўтказувчи ахлоқ формалари ва баъзи ахборот ёндашувларини ўзгартириш керак бўлади. Ахборот хавфсизлигига ўитиш ва ўзгаришларни бошқариш US SP 800-16 (Ахборот технологиялари хавфсизлигини таъминлаш соҳасида кадрларни тайёрлаш

бўйича талаблар) ҳужжатида аниқлаштирилган.

3.1-жадвал. Ахборот хавфсизлиги соҳасида авария ва бузилишларни олдини олишда ҳамкорлик (мисол).

3.1-жадвал.

Сектор	Координициялаш
Давлат ташкилотлари	• Мониторинг бўйича агент: тармоқни узлуксиз мониторинги ва хавфсизликка таҳдидларни олдиндан аниқлаш • Йиғиш бўйича агент: хавфсизлик бўйича сайтлар ва ҳалқаро ташкилотлар билан ахборот алмашинуви • Ўқув муассаси: ахборот соҳасида авариялар ва бузилишларга қарши тезкор ҳаракат имконияти ва қобилиятини ривожлантириш учун даврий моделли ўқитиш
Хусусий ташкилотлар	• Интернет хизматини етказувчи, хавфсзлик назорати ва антивирус дастурлари ишлаб чиқиш бўйича компания: трафик статистикаларини бериш, ҳужум турлари бўйича ахборот ва «червлар»/вируслар ҳақида маълумот
Ҳалқаро ташкилотлар	• Ҳужум турлари бўйича ахборот ва «червлар»/вируслар ҳақида маълумот ва шу турдаги хабарлар

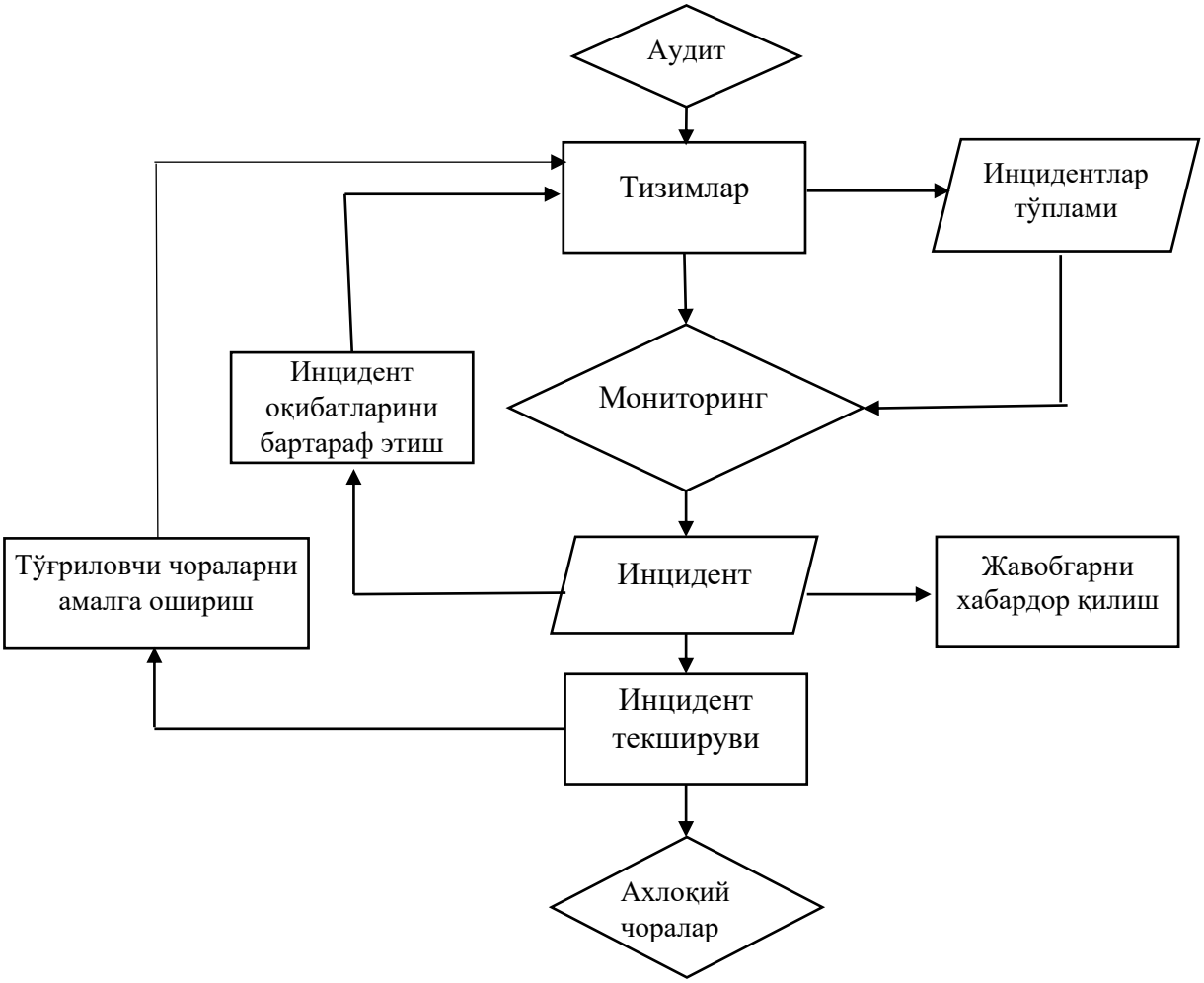
Ахборот хавфсизлиги инцидентларининг классификацияси

Ҳар бир инцидент кўплаб белгилар бўйича классификацияланиши мумкин:

- инцидентни пайдо бўлиш сабаби (чегаравий қийматга эришиш, аппарат ишдан чиқиши ва бошқалар);
- инцидент ҳаракатга олиб келувчи объект (ахборот активи, тизим ёки тизимоститизим ва бошқалар);
- инцидент муҳимлиги;
- инцидент манбаи;
- даврийлик (аввл бўлган ёки биринчи бўлиши);
- зарар (инцидент содир бўлиш моддий жиҳатдан).

Инцидентларни бошқариш жараёни.

Инцидент тизим (реал ёки потенциал) иш фаолиятига зарар етказиши сабабли жараён бошқарувини у ташкил этгани мақсадга мувофиқ. У қуйидагилардан иборат (3.2-расм):



3.2-расм. Инцидентларни бошқариш жараёни схемаси

- Инцидент ҳисобланувчи ҳодисаларни аниқлаш. Бу барчасини жорий ҳолатни бузувчи хавфлар ва ишчи ҳолатини аниқлаб, мавжуд тизим таҳлил қилиб амалга ошириш матиққа тўғри келади.
- АХИ содир бўлиш фактларини аниқлаш. Тизим мониторингини амалга ошириб, ҳодисаларни таҳлил қилиб ва йиғиб инцидентларни аниқлаймиз.
- Инцидент ҳақида жавобгар шахсни хабардор қилиш. Бу ерда ҳисобот формати, хабардор қилиш методи ва яна инцидент ҳақида хабар қилувчи шахсни алоқа маълумоти зарур.
- Инцидент сабаби ва оқибатини бартараф этиш тартиби. Аслида бу жараён олдинги этап билан бир вақтда бошланиши кера.

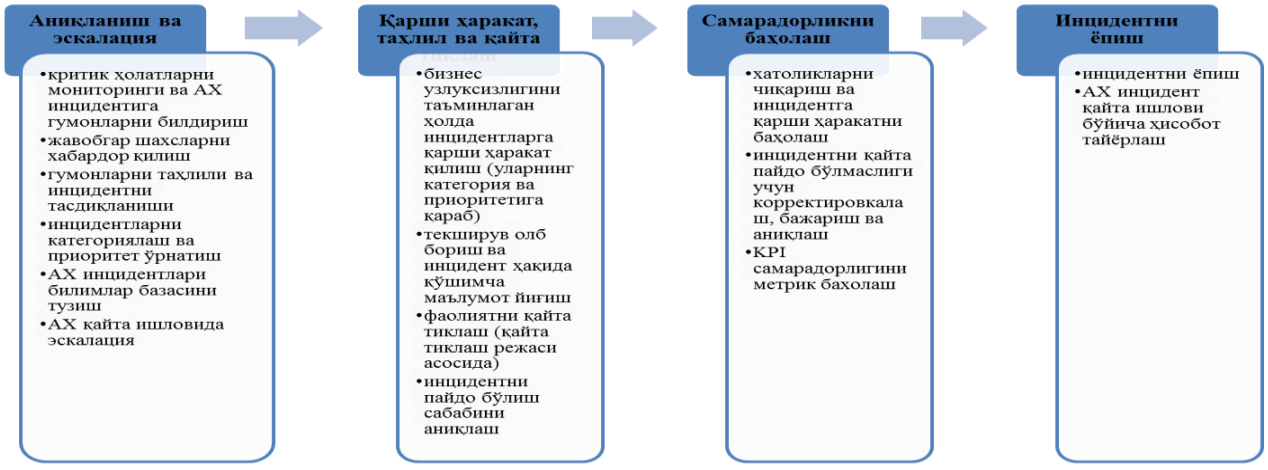
- Инцидентни текшириш тартиби. Бу ерда инцидент сабаби, инцидент содир бўлишига айбдор, йиғиш тартиби ва далилларни сақланиши. Бу этапда жавобгарликка тортиш ҳақида қарор қабул қилинади.
- Ахлоқий чоралар кўриш.
- Керакли тўғриловчи ва олдини олувчи чоралар амалга оширилади.

Инцидентларни бошқариш жараёнида жорий жараённи нормал ишлашини таъминлаш учун ваколатлар, ресурслар ва мажбуриятларга эга шахс бўлиши керак.

Инцидентларни бошқариш жараён эгасига қуйидаги ресурс ва ваколатлар берилади:

- тизимни мониторинг қилиш имкониятлари;
- инцидентлар текшируви;
- ахборотни етказиб бурувчи ва юқори эҳтимоллик билан қарши ҳаракат имконияти билан содир бўлган инцидентлар бўйича бўлимлардан ахборот олиш имконияти;
- форс-мажор инцидент оқибатларини тўғрилаш бўйича ваколатли керакли органларни мутахассисларни жалб қилиш;
- тўғриловчи чоралар яратиш имконияти.

Ахборот хавфсизлиги инцидентларини бошқариш жараёнлари автоматлашган ва тўлиқ интеграллашган бўлиши лозим (3.3-расм).



3.3-расм. Ахборот хавфсизлиги инцидентларини бошқариш жараёнларининг вазифалари

Инцидентларни бошқариш жараёнини амалга оширишнинг қийинчилиги

Инцидентларни бошқариш жараёни баъзи қийинчиликлар билан боғлиқ:

- Жараёнда ролларни аниқлаштириш. Агарда жараён эгалик бўлимида роллар етарлича аниқламтириб олинмаган бўлса, жалб қилинувчи бўлимда ҳар доим савол пайдо бўлади: ким ва қандай қарши ҳаракат қилиши ва қандай чоралар қўриши керак? Бусиз инцидентга тезкор қарши ҳаракат ва унинг текшируви қийинлашади.
- Турли манъбалардан маълумот йиғиш. Улкан кўплаб ҳимоя воситалари ва бутун тизим ўзининг турли форматли журналини олиб боради. Ҳужум векториниқуриш имконияти билан ҳодисалар корреляцияини ўтказишда барча ҳодисаларни кўриб чиқишни тақазо этади.
- Ресурсларни чекланганлиги. Ресурслар (кадрлар ва технологик) пул туради ва агарда кадрлар ресурси жараёнлар автоматизацияси орқали ечилса, керакли инфраструктурасиз бунинг иложи йўқ.
- Жорий тўсиқлар аҳамиятли, аммо ечимлидир. Ўлардан исталгани турли ташкилий тадбирлар орқали бартараф этилиши мумкин.

Фойдаланилган адабиётлар

1. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. М60 Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 170 с.
2. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари
3. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар

4. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

5. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

6. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

4-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларини идентификациялаш ва баҳолаш мезонлари

Режа:

1. Ахборот хавфсизлиги инцидентларини пайдо бўлиш сабаблари.
2. Инцидентлар факторлари.
3. Ахборот хавфсизлиги инцидентларини идентификациялаш ва баҳолаш мезонлари.
4. Инцидентлар таъсирларини камайтириш.

Ахборот хавфсизлиги инцидентларини пайдо бўлиш сабаблари

Ахборот хавфсизлиги сиёсатлари ёки бошқарув воситалари ўз-ўзидан ахборот, ахборот тизимлари, хизматлар ёки тармоқларнинг тўлиқ ҳимоясини кафолатламайди. Бошқарув воситалари жорий қилингандан сўнг қолган заиф нуқталар ахборот хавфсизлигининг самарадорлигини камайтириши ва натижада ахборот хавфсизлиги инцидентларини вужудга келтириши эхтимоли мавжуд. Потенциал равишда бу холат ташкилотнинг фаолиятига бевосита ва билвосита салбий таъсир кўрсатиши мумкин. Бундан ташқари олдиндан маълум бўлмаган янги хавф-хатарлар албатта вужудга келади. Ташкилотинг бундай инцидентларга қарши курашиш учун етарли

тажрибасининг йўқлиги ҳар қандай жавобнинг самарадорлигини пасайтиради ва ташкилот фаолиятига салбий таъсир кўрсатади.

Ахборот хафсизлиги инцидентлари олдиндан режалаштирилган ёки тасодифий бўлиши (масалан, хато ёки табиий офат туфайли юзага келган) бўлиши ҳамда техник ёки физик омиллар таъсирида рўй бериши мумкин. Уларнинг натижаси маълумотни рухсатсиз ошкор қилиш, ўзгартириш, йўқ қилиш ёки маълумотни ишлатиб бўлмайдиган ҳолатга келтириш, ташкилот активларига зиён етказиш ёки уларни талон-тарож қилиш бўлиши мумкин.

Ахборот хавсизлигини техник инцидентлари(аномал тармоқ фаоллиги, хизматнинг ишдан чиқишига мўлжалланган ҳужумлар, рухсат этилмаган маълумотни қўлга киритишга уриниш, зарарли кодни юклаш ва ҳакозо) автоматик аниқланиши мумкин, масалан, назорат ёзувлари таҳлили қурилмалари, тармоқлараро экранлар, ҳужумларни аниқлаш тизимлари, зарарли кодларни аниқлашнинг инструментал воситалари (антивируслар) томонидан юбориладиган огоҳлантириш сигналлари бўлиши мумкин.

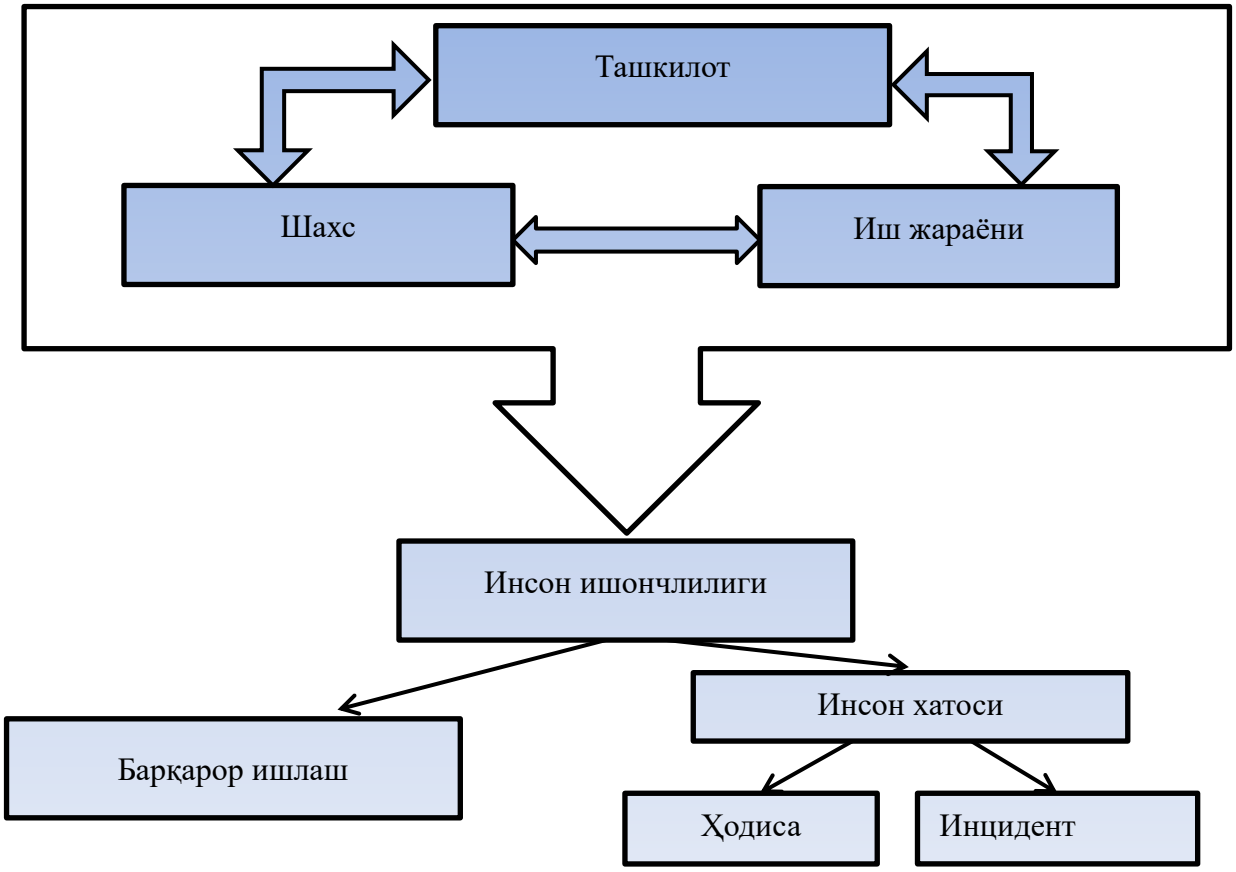
Инцидент факторлари

Бугунги кунга ташкилотларни ахборот тизимисиз тасаввур қилиш қийин. Бу эса ўз навбатида ташкилотдаги активларни бутунлигини, махфийлигини ва ҳақиқий эканлигини таъминлаш зарурлигини билдиради ва натижада ахборот хавфсизлигини бошқарув тизимини (АХБТ) ташкил этишни белгилайди. АХБТ ни мустаҳкам хавфсилик асосларини белгилайди, ахборот технологиялари ресурсларидан тизимли тарзда фойдаланишни тартибга солади. Лекин АХБТ даги техник ўзгаришлар ҳам ресурлардан фойдаланиш учун қулай муҳитни яратмайди. Қулай муҳитни яратиш инсон фаолияти билан узвий боғлиқдур.

Ахборот хавсизлигида инсон омили муҳим рол ўйнайди. Бугунги кунга келиб инцидентларни турли кўринишларда учратиш мумкин. Инцидентларни юзага келиш сабаблари ҳам турлича. Аксарият инцидентлар инсон омили натижасида юзага келади. Бунга асосий сабаб сифатида ахборот технологияларидан фойдаланувчиларни етарли даражада билимга эга

эмалисликлари ва социал инжинериянинг жуда юқори суратларда ривожланиши ахборот хавфсизлигида юқори даражадаги инцидентларни келтириб чиқарди.

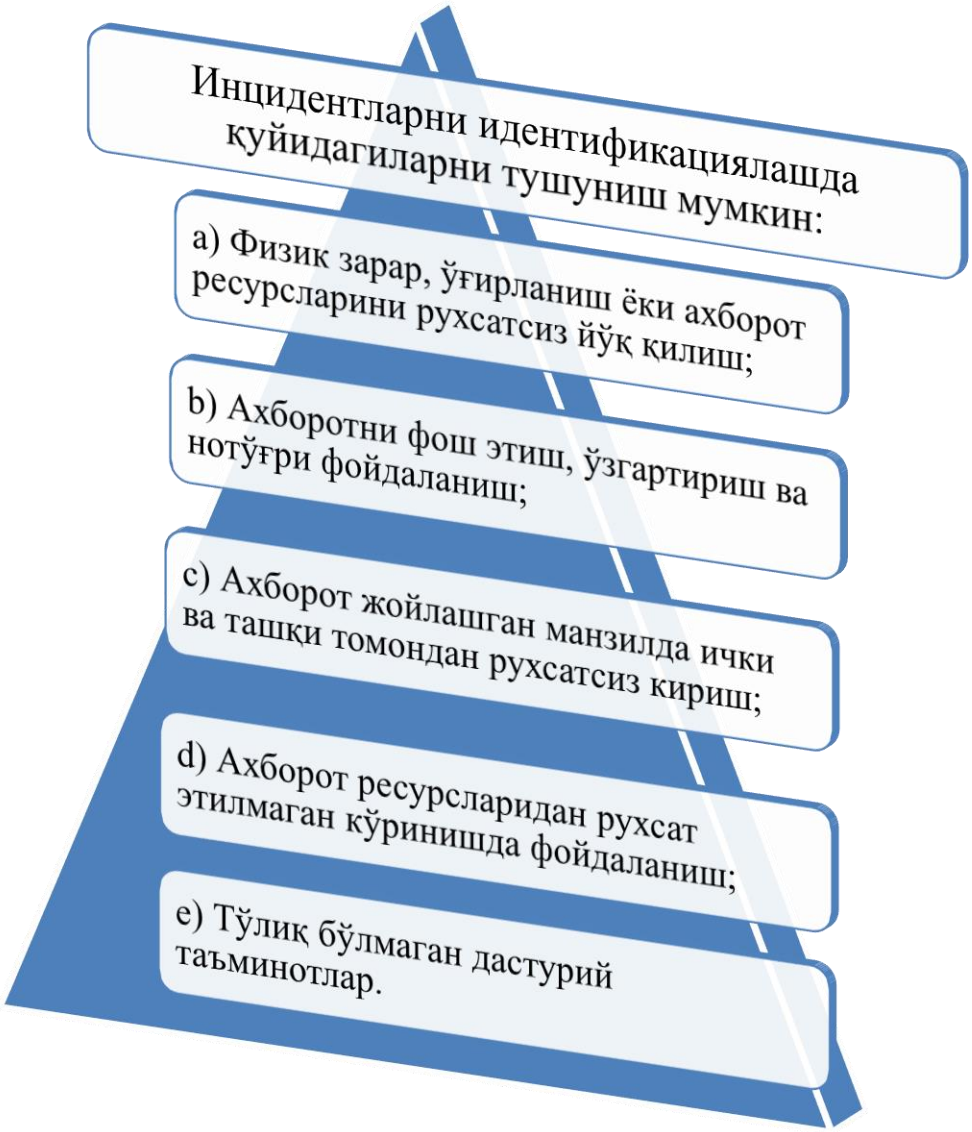
Кўплаб ахборот технологиялари ташкилотлари инцидентларга жавоб чоралари ҳамда малакали ходимларга эга бўлсада бу ташкилотлар ахборот хавфсизлиги инцидентларини бошқаришлари мураккаб жараён ҳисобланади. Биринчи вазифа малакали мутахассисларга эга бўлиш, иккинчиси эса инцидентларга қарши чора тадбирларни ишлаб чиқиш ҳисобланади. Ташкилотнинг барча ресурсларидан фойдаланган ҳолда инцидентларни аниқлаш ва инцидентлар ҳақида ҳисобот тайёрлаш, бошқариш учун омил ҳисобланади. Инцидентларни аниқлашни автоматлаштирилган тизимларини ҳосил қилиш ва шу билан бирга реал вақтда жавоб чораларини кўришни ташкиллаштиришни амалга оширилиши лозим. Янги ахборот тизимларида хавфсизлик инцидентларини автоматик аниқлаш тизмини ривожлантириши учун, тез-тез профилактика ишларини амалга оширилиш мақсадага мувофиқ.



4.1-расм. Инцидент факторларида инсон омили

Ахборот хавфсизлиги инцидентларини идентификациялаш ва баҳолаш мезонлари

Ахборот хавфсизлиги инцидентларини идентификацияловчи ташкилотлар мавжуд бўлиб улар қўшимча чоралар, тегишли тузатишлар ва зарур бўлса такрорланиш эхтимолини камайтириш тартибларини кўриб чиқади. Корпаратив Ахборот Хавфсизлиги Идораси (CISO) КАХИ мана шундай ишларни амалга оширади. Инцидентларни идентификациялаш деганда қуйдагиларни тушуниш мумкин:



4.2-расм. Ахборот хавфсизлиги инцидентларини идентификациялаш жараёни

Инцидентларини баҳолаш ва қарор қабул қилиш мезонлари

Ахборот хавфсизлигида маълумотларни ҳимоя қилиш кўлами жуда кенг.

Шу сабабли вақти-вақти билан баҳолашларни амалга ошириш, инцидентларни бошқариш қобилятларини такомиллаштириш муҳим аҳамият касб этади. Инцидентларни бошқариш қуйидаги босқичларни ўз ичига олади:

4.3-расм. Инцидентларини баҳолаш ва қарор қабул қилиш мезонлари

Баҳолаш ва қарор қабул қилиш босқичи учун ташкилотлар қуйдаги чора-тадбирларни таъминлаши лозим:

a) Ходиса ахборот хавфсизлиги инциденти сифатида ёки ёлғон сифатида қабул қилиниши, агар ёлғон бўлмаса босқичма-босқич кенг ўрганилиши лозим;

b) ҳодисанинг ахборот хавфсизлиги инциденти сифатида таснифланишини аниқлаш мақсадида ахборот хавфсизлиги инцидентларига қарши кураш хизмати (АХИҚКХ) томонидан бахо берилишидир. Ахборот хавфсизлиги инциденти қандай, ким томонидан ва қайси кетма-кетликда қайта ишлаши ҳақида қарор қабул қилиниши лозим. Бунда таҳлил ҳар бир ахборот

хавфсилиги инцидентининг тегишли турга мансуб эканлигининг таъминлаш учун ўз ичига олдиндан белгиланган кетма-кетликлар бўйича тақсимлаш жараёнини ўз ичига олиши ва ахборот хавфсизлиги инцидентларини қайта ишлаш ва уларга жавоб қайтариш лозимлигини аниқлаш ҳамда тезкор жавоб чораларини кўриши лозим;

c) маълумотларни электрон шаклда йиғиш ва хафвсиз сақланишини ҳамда ички интизомий чораларни доимий назоратини таъминлаш.

Ахборот хавфсизлиги инцидентлари ёки заифликлари бўйича барча йиғилган маълумотлар АХИҚКХ рахбарлигидаги ахборот хавфсизлиги инцидентлари маълумотлар омборида сақаланиши керак. Хар бир фаолият тури жараёнида хабар бериладиган барча маълумотлар бахо бериш ва қарор қабул қилиш ва тегишли чоралар кўриш учун фойдаланилган омборни таъминлаш учун тўлиқ бўлиши лозим.

Ахборот хавфсилиги ҳодисаси ахборот хавфсизлиги инциденти сифатида аниқланган бўлса бахо беришнинг кейинги босқичига ўтказилади. Бунинг натижасида тузатиш ҳаракатлари, масалан, қўшимча авариявий ҳимоя чораларини аниқлаш, бошқа мутахассислардан маслаҳат сўралиши мумкин:

a) Ахборот хавфсизлиги инциденти нимадан иборат эканлиги.

b) Унинг сабаби ким ёки нима эканлиги.

c) У нимага таъсир қилиши ва қилиши мумкинлиги.

d) Ахборот хавфсизлиги инциденти ташкилот бизнесига реал ёки эхтимолий таъсири.

e) Ахборот хавфсизлиги инцидентининг муҳимлилик даражаси.

f) Ахборот хавфсизлиги инциденти бунгача қандай қайта ишланганлиги.

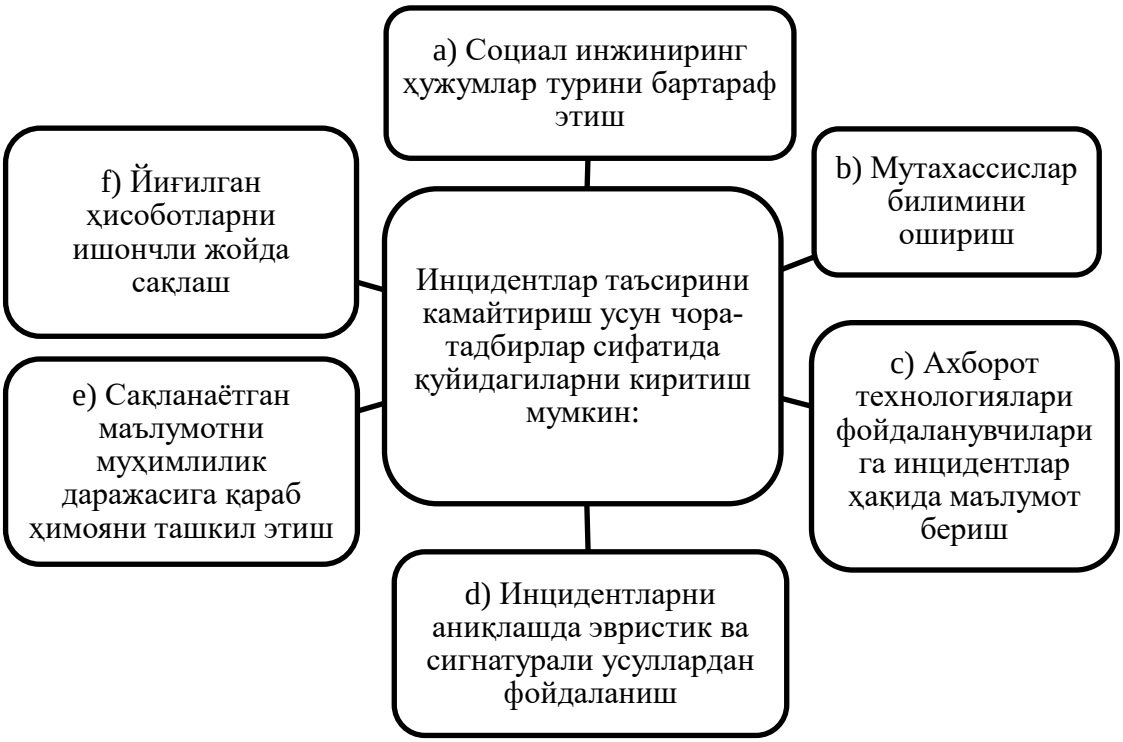
Биринчи бўлиб қуйидаги оқибатлардан қайси бири аҳамиятли эканлиги аниқланади. Масалан:

4.4-расм. Инцидентларни таъсир доирасини аниқлаш

Жараёнлар кўламининг кенгайиши инцидентларнинг муҳим элементи ҳисобланади. Қизиғи шундаки инцидентлар ташкилотнинг фаолиятидан келиб чиққан ҳолда турлича бўлади. Инцидентлар муайян шароитда фаол тизимларни ва тармоқларнинг мониторингини ўтказиш сиёсатини қилинади. Бундан ташқари маълумотларни аудитлаш ва кимдир шу маълумотларга кирмоқчи бўлса махсус рухсатномага эга бўлиши талаб қилинади. Текшириш давомида содир бўлмаган инцидентлар ҳақидаги маълумотларни кўриб чиқиш лозим бўлади.

Инцидентлар таъсирини камайтириш

Ахборот хавфсизлиги инциденнтларини таъсирини камайтириш учун биринчи навбатда уларни келиб чиқиш сабаблари ўрганилади. Яъни бу инцидентлар қандай содир бўлди, ким томонидан, атайин қилиндими ёки табиий офатми, мақсади аниқланади ва тўлиқ ҳисобот йиғилади. Мутахассисдан юқори даражадаги билим ва малака талаб этилади.



4.5-расм. Инцидентлар таъсирини камайтириш

Фойдаланилган адабиётлар

1. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. М60 Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 170 с.

2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

3. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

4. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

5-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларини қайта ишлаш ва аниқлаш

Режа:

1. Ахборот хавфсизлиги инцидентларида ҳодисаларни аниқлаб олиш ва улар ҳақида ахборот бериш.
2. Ҳодисаларни қайта ишлаш.
3. Ахборот хавфсизлиги инцидентларини бирламчи ва иккиламчи баҳолаш.

Ахборот хавфсизлиги инцидентларида ҳодисаларни аниқлаб олиш ва улар ҳақида ахборот бериш

Ахборот технологияларининг тадбиқ этилиши ташкилот ва муассасаларда иш олиб бориш услублари ўзгарди. Ахборот технологиялари олиб кирган ўзгаришлар натижасида функционал жараёнларни автоматлаштиришга эришилди. Лекин ахборот технологияларидан фойдаланиш илгари маълум бўлмаган хавфларни келтириб чиқарди. Юқори технологияларнинг соҳага тадбиқи натижасида ҳар қандай турдаги корхона фаолиятига кибержиноятчиларнинг аралашишига имкон туғилди.

Корхона ишига бу тарзда аралашишнинг бир неча сабаблари бор, одатда бузғунчилар пулларни ўғирлашга ҳаракат қиладилар, лекин баъзи ҳолларда эса улар корхона обросига путур етказиш мақсадида ёки махфий маълумотни ўғирлаш учун бу ишни амалга оширадилар.

Ахборот хавфсизлигига рахна солувчи турли инцидентлар мавжуд. Энг кўп тарқалганлари бу: DDoS-ҳужумлар (“хизмат кўрсатишадан воз кечишга ундайдиган ҳужумлар”), масофадан банк хизматларидаги фирибгарлик (МБХ), серверларни бузиш ва конфиденциал маълумотларни ўғирлаш, корпоратив маълумотларни ўғирланиши, Интернет тармоғида корхона обрўсига путур етказувчи миш-мишларни жойлаштириш. Юқорида саналган ҳар бир инцидент талофат кўрган корхоналар обрўсига зарар етказади.

Ҳозирги кунда корхоналарда ташқи ва ички характерга эга бўлган ахборот хавфсизлиги инцидентлари содир бўлмоқда.

Ички инцидент – зарар кўрган томон билан бевосита (меҳнат шартномаси) боғлиқ бўлган шахс томонидан амалга оширилган инцидент. Тизимда содир бўлиши мумкин бўлган қуйидаги тез-тез учраб турадиган ҳолатларни келтириш мумкин:

- конфиденциал маълумотларни ўғирланиши;
- ахборотга рухсат этилмаган кириш;
- маълумотларни ўчириш;
- корхона активларини шахсий мақсадларда ёки фирибгарлик учун фойдаланиш;
- қўпорувчилик;
- тармоқдаги ғайритабий фаоллик;
- ғайритабий бизнес шартномалар;
- ахборот технологиялари ёрдамида фирибгарлик.

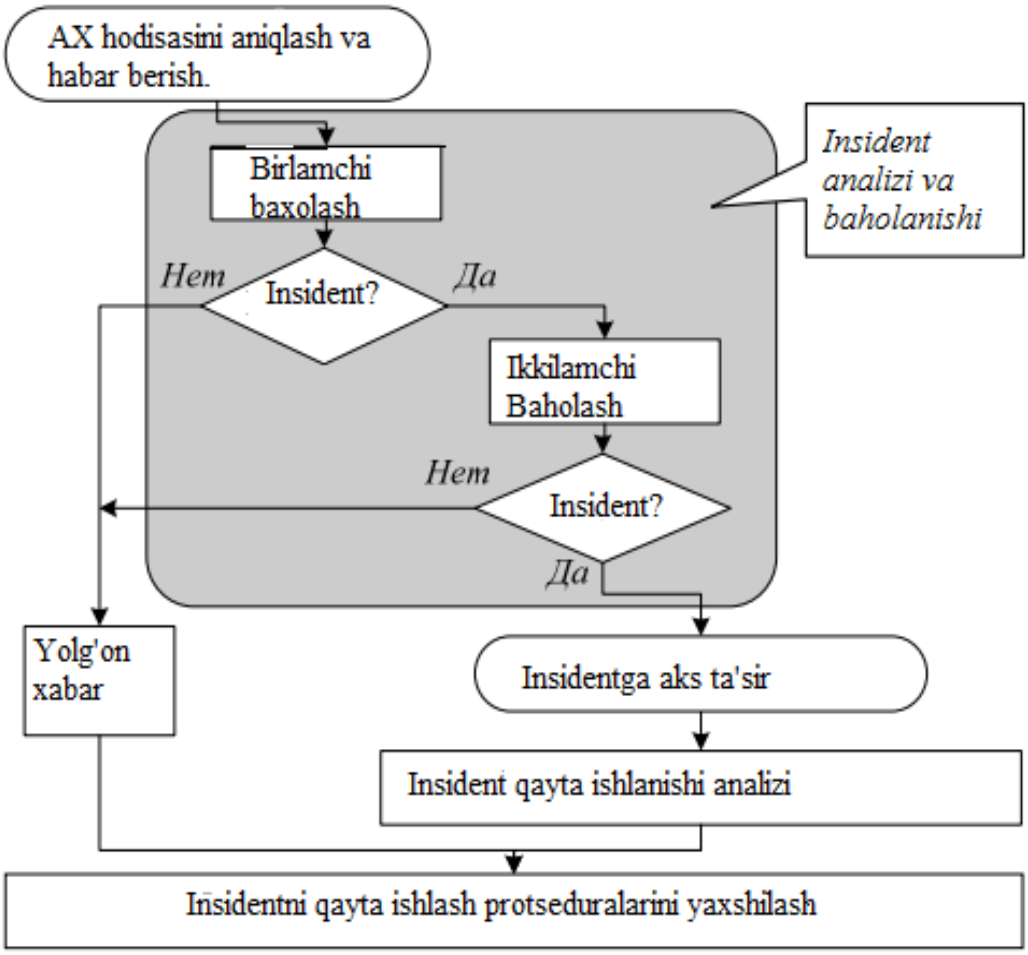
Ташқи инцидент – бу зарар кўрган томон билан ҳеч қандай боғлиқлиги бўлмаган шахслар томонидан уюштирилган инцидент. Тизимда содир бўлиши мумкин бўлган қуйидаги тез-тез учраб турадиган ҳолатларни келтириш мумкин:

- МБХ тизимларидаги фирибгарлик;
- DDoS ҳужумлар;
- трафикни қўлга олиниши ва алмаштириб қўйилиши;
- корхона брендидан Интернетда нотўғри фойдаланиш;
- Фишинг;
- корхонанинг конфеденсиал маълумотларини Интернет тармоғига жойланиши;
- бузиб кириш, бузиб киришга уриниш, корхона порталини сканерлаш;
- тармоқни сканерлаш, тармоқ тугунларини сканерлашга уриниш;
- вирус ҳужумлари;

- конфеденсиал маълумотларга рухсат этилмаган кириш;
- ғайритабиий хатлар (тажовузкор хатлар).

Ҳодисаларни қайта ишлаш

Ахборот тенологиялари ва компьютер тармоқларининг ривожланган сари ахборот хавфсизлиги инцидентлари сони ҳам ошмоқда, улар АХ тизими фаоллигига рахна солиб кўнгилсиз ҳолатларга олиб келиши мумкин. Буларга мисол қилиб, конфиденциалликни бузилишини, ахборот активларининг яхлитлигини бузилиши ва бизнес жараёнларнинг узилиб қолишини келтириш мумкин. Ахборот хавфсизлиги инцидентларини қайта ишлашини бошқариш 5.1-расмда келтирилган.



5.1- расм. Ахборот хавфсизлиги инцидентларини қайта ишлашини бошқариш

Халқаро ISO 27001:2005 стандарти ахборот хавфсизлиги инцидентларини бошқариш процедурасини яратишга алоҳида урғу беради – маълумки, содир бўлиши мумкин бўлган инцидентларнинг олдини олиш,

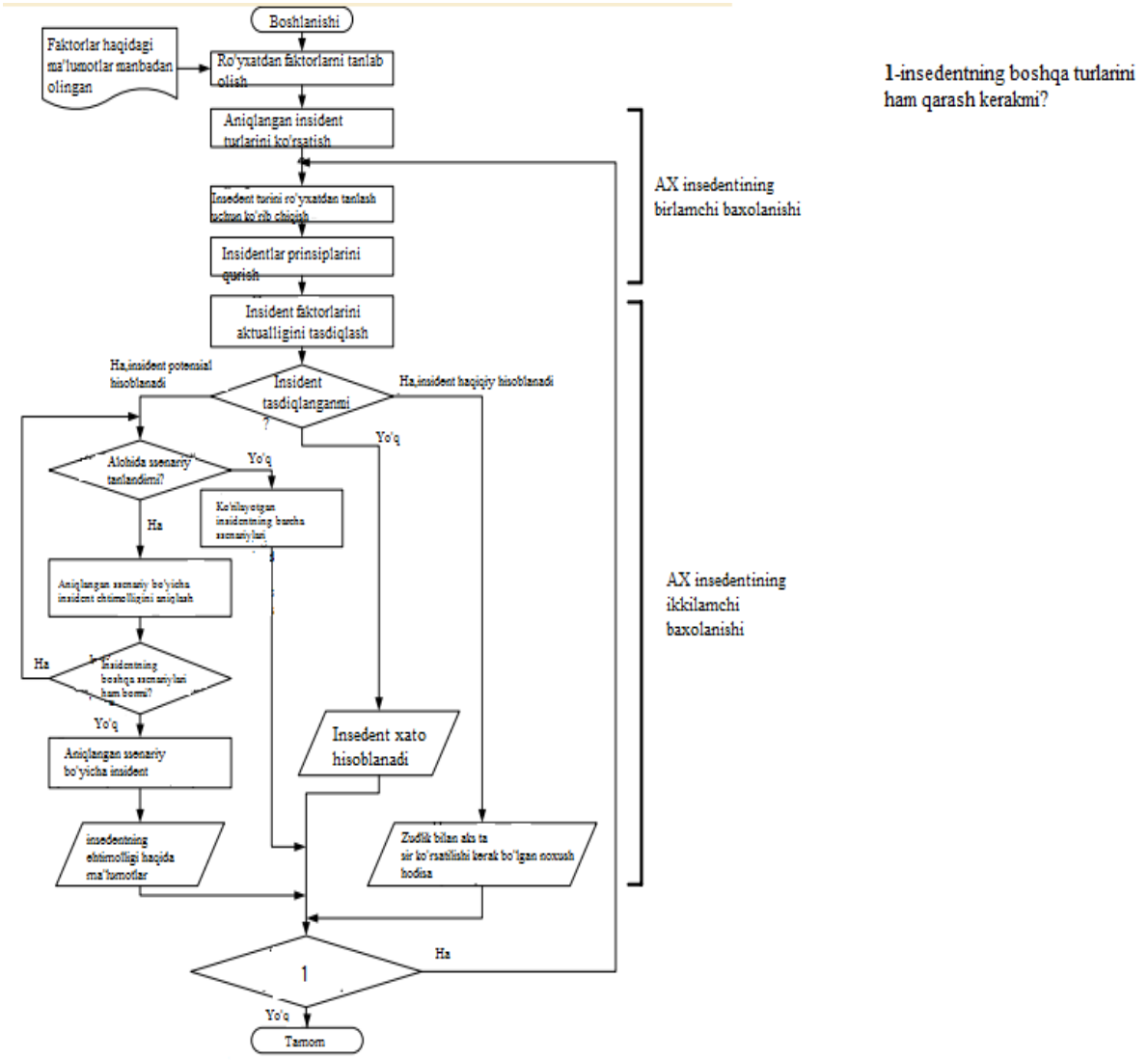
инцидентлардан кейинги келадиган талофотларни тузатишдан кўра анча самарали ҳисобланади. Халқаро ISO/IEC 2705 ва миллий ГОСТ Р ИСО/МЭК 18044:2007 стандартларда инцидентларни бошқариш жараёнлари келтириб ўтилади. Норматив ҳуқуқий ҳужжатлар ва ресурслар ҳақидаги саволлар кўрилади, бу жараёнларни амалга ошириш бўйича тушунтириш ва тавсиялар берилган.

Ахборот хавфсизлиги инцидентларини бирламчи ва иккиламчи баҳолаш

АХ ҳодисасини аниқлаш, таҳлил қилиш ва баҳолаш инцидентларни бошқаришда муҳим босқичлар ҳисобланади, чунки бу босқичларда олинган хабарнинг муҳимлилиги ва ишончлилиги инцидентга қарши чора кўришда қарор қабул қилишда муҳим рол ўйнайди. Инцидентларни аниқлаб олиш жараёни улар ҳақида кам маълумот борлиги билан ҳам мураккаблашади.

Бирламчи баҳолашда АХ ҳодисасини АХ инциденти сифатида аниқлашда маълум бир инцидент турига ишора қилувчи ҳодисаларга асосланади. АХ ҳодисаси фактори - АХ ҳодисасининг АХ бузилган ҳолатига ёки хавфсизлик чораларига бўлган таҳдидга ишора қилувчи белгиси, шунингдек бунгача номаълум бўлган хавфсизликка таҳдид солувчи ҳолатлар ҳам тушунилади.

Юқорида келтирилган алгоритмда иккиламчи баҳолаш функцияси ҳам киритилган бўлиб, унда кўрилаётган инцидент долзарблигини тасдиқлаш мақсадида қўшимча маълумотлар тўпланади. Ҳар бир кўрилаётган ҳодиса учун уни инцидент сифатида қабул қилиш учун ёки бу нарсани рад этиш учун зарур бўлган маълумотлар ва шу маълумотларнинг манбаси бериб борилади. Иккиламчи баҳолашда инцидент факторларидан келиб чиққан ҳолда алгоритм унинг сценарийсини ўзгартириб боради. Бундан ташқари алгоритм келтириб ўтилмаган факторларга асосланган инцидент сценарийларини ҳам қуриш имконини яратади.



5.2-расм. Инцидентларини бирламчи ва иккиламчи баҳолашини амалга ишлаш алгоритми

Бу функсия инцидентларни қайта ишлашида АХ инциденти ҳақида қўшимча маълумотлар йиғишни ва олинаётган маълумотларнинг ишончлилигини оширишга ҳамда келгусида АХ инцедентларига бўлган акс таъсири тезлигини оширишда қўл келади. Алгоритм потенциал инцидентнинг алоҳида сценарийлар бўйича қараб чиқишни ва хавфсизлик учун муаммо бўладиган кўнгилсиз ҳолатларни бартараф этиш имкониятини беради. Шунинг учун алгоритм 5 та поғонали хавфсизлик поғонаси ўрнатилган-0 дан (хавфсизлик чоралари йўқ) 4 гача (инцидент сценарийси бўйича кўнгилсиз ҳодисаларнинг бартараф этишга қаратилган хавфсизлик чоралари).

Фойдаланилган адабиётлар

1. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 170 с.

2. Межрегиональная общественная организация «Союз ИТ-директоров» Межрегиональная общественная организация «Ассоциация руководителей служб информационной безопасности» (АРСИБ) разработано при участии Group-IB и LETA Инциденты информационной безопасности Рекомендации по реагированию Москва 2011.

3. С. Л. Зефиров, А. Ю. Щербакова. Оценка инцидентов информационной безопасности.

4. ISO/IEC TR 18044:2004 Information technology - Security techniques - Information security insident management (IDT).

5. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари

6. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар.

7. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

6-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларига жавоб қайтариш

Режа:

1. Ахборот хавфсизлиги инцидентларига тезкор жавоб қайтариш.
2. Ахборот хавфсизлиги инцидентларини бошқарувчанлиги.
3. Ахборот хавфсизлиги инцидентларини экспертизаси.
4. Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг техник. қўлланилиши

1. Ахборотхавфсизлиги инцидентларига тезкор жавоб қайтариш

Ахборот хавфсизлиги инцидентларига тезкор жавоб қайтаришнинг асосий мақсади инцидентнинг олдини олиш (масалан, агар чекланган руҳсат билан маълумот алмашиш блокланса) ёки эҳтимолий зарарни тезлик билан минималлаштиришдир.

Ахборот хавфсизлиги инцидентларига тезкор жавоб қайтариш ўз ичига техник чора – тадбирларни, криминал белгили маълумотлар тўлиқлигини таъминлаш ва бу маълумотларнинг тергов қилиш эҳтимоллиги, ҳамда инцидентдан кўрилувчи зарарни камайтирувчи ва ҳуқуқни ҳимоя қилувчи органлар учун ҳужжатлар таркибидан ва ташкилий чора – тадбирлардан иборат.

Техник чора – тадбирларнинг асл моҳияти маълумот бутунлигини сақлаш, инцидентга потенсиал алоқа, ўчириш ё`ллари, аборот сақловчи мавжуд қурилмаларни ҳимоялаш ва сақлаш. Ахборот қурилмасини ўчириш бузғунчи ҳаракатлар ва зараркунанда дастурларнинг натижасида криминал яширин маълумотларни йўқ қилиш эҳтимоллигини нолга тушуради, уларни беркитиш, белгилаш ва кераклича сақлаш тергов жараёнларида кераклича даражада аниқ натижаларни тақдим этади.

Ташкилий чора – тадбирлар ташкилот раҳбариятини огоҳлантириш, ташкилот бўлимлари ахборот хавфсизлиги ва уларни қизиқтирувчи инцидент ҳақидаги фактларни ўз ичига олади. Ташкилий чора – тадбирларни ўтказиш тўғрисидаги ҳужжатлар жиноий ишлар бўйича терговда ёки сўроқларни йўқ

қилишда қайта кўриб чиқиш учун саволларга асосланган ҳолатда, ташкилот ахборот қурилмаларини тергов жараёнларига рухсатини бегилайди.

Ахборот хавфсизлиги инцидентларига жавоб қайтарилгач инцидентнинг таҳлили ва ташкилот ахборот тизимини қайта тиклаш бошланади. Ташкилот ахборот тизимини тиклаш ажратилган ва белгиланган қурулмаларни янгиларига алмаштиришни, керакли ДТ ларни ўрнатишни ва ахборот хавфсизлиги етарлича таъминлаш учун ахборот тизимининг қайдларини созлашни ўз ичига олади.

Ҳужум инцидентлари ҳаракатларининг умумий алгоритмлари

Ахборот хавфсизлиги хизматининг асосий вазифаси – бу корхона учун бизнесда мавжуд усуллари, формулалашган, аниқ ё`лни белгиловчи ва махфийлашган Ахборотларга алоқадор зарар етиши ёки йўқотилиши мумкин бўлган ахборот хавфсизлигига бўладиган хавф – хатарларни олдини олиш.

Ахборот хавфсизлиги соҳасида корхона мажбуриятлари, барча умумий принсип ва ҳуқуқлар, корхона учун режалаштирилган мавжуд ва формал режалар “Ахборот хавфсизлиги сиёсати” ҳужжатида келтирилади. Ушбу ҳужжатда хавфсизлик ҳодимларининг ахборот хавфсизлигига инцидент хуружи амалга ошганда қандай ҳаракатларни амалга ошириши аниқ ва қадамма – қадам келтирилади.

Ахборот хавфсизлигини бузишдаги одатий ссенарийлар қуйи базавий ҳаракатларни амалга оширишга асосланган бўлиши мумкин. Ахборот хавфсизлиги инциденти жараёнида қуйидагиларни амалга ошириш зарур:

1. инцидентни идентификатсиялаш ва у шу ерда амалга оширилганига ишонч ҳосил қилиш.

2. амалга ошаётган инцидентда АТ – инфраструктурасини локалластириш.

3. мавжуд инцидентга, обектларга мурожаат ҳуқуқини чеклаш.

4. қайд ёзувларини инцидентларга жавоб қайтариш бўлими раҳбари номига расмийлаштириш.

5. консултатсия учун малакали муассисларни жалб қилиш.

6. инцидентларни таҳлилловчи гуруҳни йигиш ва далилларни тўплаш ва тизимни тиклаш бўйича иш режасини тузиш. Барча ҳаракатларни, шу жумладан инцидентларга жавоб қайтариш усулларини протоколлаштириш.

7. далилларни сақлаш ва керакли ўтказмаларни таъминлаш.

7.1. Энергияга боғлиқ ахборотларни ишчи тизимлардан узиш.

7.2. реал вақтда инцидент ҳақидаги ахборотларни йиғиш.

7.3. қувват тизимидан узиш.

8. учинчи мустақил томонни базавий далил сифатида ахборот қурилмаларини белгилаш, намуналарни олиш ва ахборотларни кейинги таҳлил ва сақлаш учун киритиш.

8.1. ахборот қурилмаларидаги барча операцсиялар протоколларини расмийлаштириш.

8.2. обект ҳақидаги маълумотларни яратиш, унга алоқадор маълумотлар, ҳатто уларнинг сақланиш жойларини ҳам.

8.3. жараёнларни фото ёки видео камераларга ёзиш.

8.4. чоп этилган обектларни протоколлар билан биргаликда ва ишончили жойда сақлаш зарур токи улар таҳлил учун ёки ҳуқуқни муҳофаза қилувчи органларга етказилмагунига қадар.

9. жорий далилларни сақлаш ва етказиш амалга оширилгач Ахборот тизимининг ишчи ҳолатини тиклаш лозим.

10. таҳлил олиб борилаётганда далилларнинг ўзгармаслигини таъминлаш. Бунда фақат нусхалар билан ишлаш зарур.

11. изланишлар олиб борилаётганда ишларни махсус бўлимлар ва тегишли ташкилотлар билан ҳамкорликда олиб борилиши керак (масалан ахборот хавфсизлиги инцидентларини таҳлиллаш ва ахборот хавфсизлиги ни таъминлаш бўйича корхоналар).

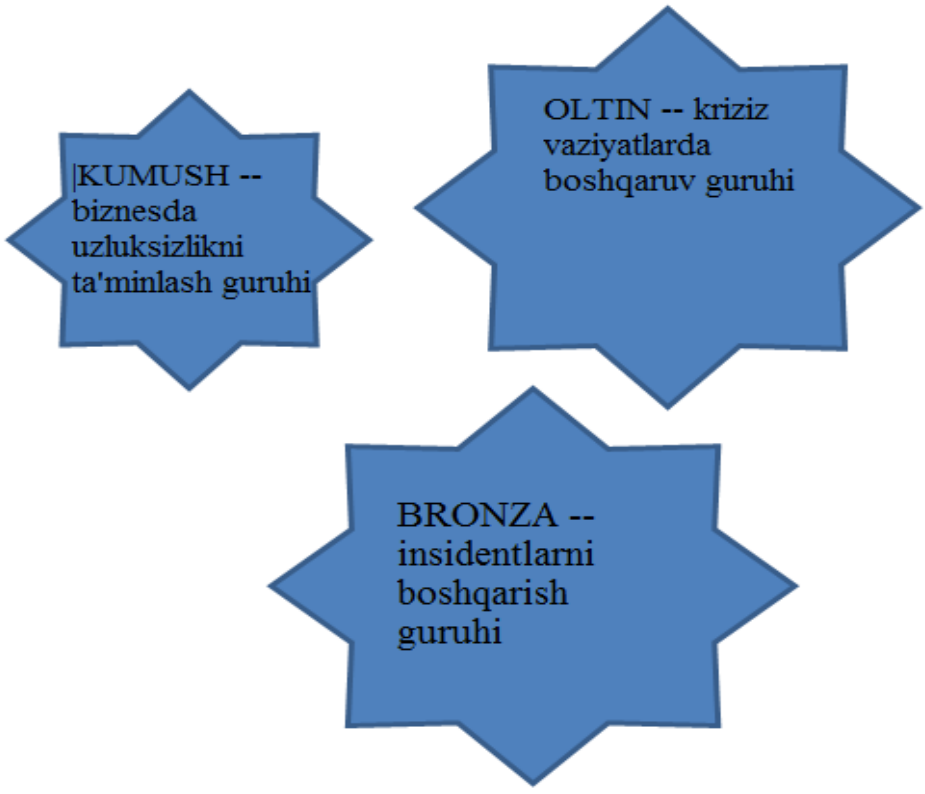
12. таҳлиллар тугагач мавжуд ҳисоботни тайёрлаш ва келажакда инцидентни йўқ қилиш ва такрорланмасилги таъминлаш учун тавсиялар киритилади.

13. ҳуқуқни муҳофаза қиливчи органлар билан ҳамкорликда ишлаганда

уларга инцидент ҳақида батавсил маълумот бериш лозим. Яъни барча далиллар ва анализ натижалари.

2. Ахборот хавфсизлиги инцидентларини бошқарувчанлиги

Ахборот хавфсизлиги инцидентларини бошқариш тизимида рўйҳатга олиш, тезкор жавоб қайтариш ва Ахборот хавфсизлиги инцидентларига руҳсат, ҳамда инцидентлар билан ишлашнинг барча сикли ташкиллаштирилади. Қанча тез ва қониқарли даражада корхона мавжуд ахборот хавфсизлиги инцидентларига жавоб қайтара олса бу зарар миқдорига боғлиқ бўлади, унинг натижаси олдиндан маълум бўлади. Шунинг учун инцидентга руҳсатга тайёргарлик муҳим аҳамиятга эга. Тайёрланиш жараёни режалаштириш, жавобгар шахсни белгилаш, мажбуриятларни тақсимлаш инцидентларни бошқариш бўйича режаларни ишлаб чиқишни ўз ичига олади.



6.1-расм. Инцидентларни бошқариш структураси (PAS 77:2006)

Ахборот хавфсизлиги инцидентларини бошқариш жараёни фақатгина рухсат бериш эмас, балки уларни таҳлил қилиш, рухсат эффиктивлигини таъминлаш ҳам муҳим. Ишлаб чиқилган режаларни ишчи муҳитнинг қўллаб – қувватлашига тестлаш ва модификатсилаш керак. Бундан ташқари кучсиз

инцидентларни ҳам мавжуд ҳимоя тизимининг даражасини аниқлаш ва ўзгаришлар киритиш учун ҳам таҳлил қилиш талаб этилади. Агарда анализ даврида инцидентнинг ўхшаш нусхалари аниқланса, мақбул ҳаракатлар такрорланади. Агарда тизим хатоликлари аниқланса белгиланган режалар натижа бермаса, унда тайёргарлик босқичига ўтилади.

- Олтин – МЧС, ИИВ, авария хизматлари ва органлари томонидан қўллаб – қувватловчи, юқори менежмент ташкилотлари,
- Кумуш – хавф – хатарларни ва бизнесдаги узулишлар бошқариш хизмати.
- Бронза – АТ ва Ахборот хавфсизлиги марказлари, кадрларни қўллаб қувватлаш, юристлар, техник хавфсизлик ва ҳуқуқни муҳофаза қилиш органлари

Муаммолар.

Антивируслар, тармоқлараро экранлар, МББТ лар, web-сервислар, заифликлар сканерлари ва ҳимоянинг бошқа воситалари ахборот хавфсизлиги – инфраструктурасини тўла ифодалай олмайди. Ҳимоянинг барча элементлари алоҳида созланади ва ишлайди, лекин улар орасида ўзаро алоқадор жойи йўқ. Айнан шу ҳимоя комплексини самарадор ишлашини, инцидентларни аниқлашнинг максимал тезлигини таъминлайди.

Ахборот хавфсизлиги нинг марказлашмаган ҳодисалари мониторинг муаммолари:

- Ахборот хавфсизлиги инсдентларига тезкор жавоб қайтариш;
- Хавф манбаини аниқлай олмаслик ва мазкур инцидентга жавобгарни топиш;
- Енг мушкул томони реал вақт режимида инсдент ҳақида тўлиқ ва ишончли ахборот олиш.
- Аудиторнинг ахборот хавфсизлиги ҳодисаларини сертификатлаш ва текширувларни осон таҳлил қилишни ташкиллаштириш.

Ечимлар.

Ахборот хавфсизлиги соҳасида бу муаммалорни ечиш учун дастлаб

Ахборот хавфсизлиги инцидентларини бошқариш марказини ташкил этиш лозим ва у қуйидаги вазифаларнинг ечимини топиши лозим:

- Ахборот хавфсизлиги инцидентларини аниқлаш ва уларга жавоб қайтариш вақтини минималлаштириш;
- Инцидентларни таҳлил қилишда ахборот хавфсизлиги қоидалари ва сиёсатини бажарилишини назарот қилиш;
- Ахборот хавфсизлиги ҳолатининг марказлашган мониторинггини ташкил этиш;
- Ахборот хавфсизлиги хавф – хатарларни бошқариш самарадорлигини ошириш ва ҳимоянинг керакли қўшимча чораларини кўриш;
- Корхонанинг бошқарилувчанлик ва стабиллик даражасини ошириш;
- Ахборот хавфсизлиги ҳодисалари мониторингги учун нормативе ва халқаро талабларни бажариш;
- Ахборот хавфсизлиги инцидентларини бошқариш марказини ташкил этишда унинг 3 хил асосий ё`налишларини инобатга олиш: технология, жараён ва шахс.

Технологиялар.

Технолигиялар қуйидаги гуруҳларга бўлинади:

- Аудит ҳодисалари;
- Ҳодисаларни йиғиш, филтрлаш, сақлаш;
- Ҳодисалар такрорланиши ва инцидентларни аниқлаш;
- Инцидентлар таҳлили ва муаммоларни гуруҳлаш;
- Инцидентларни бошқариш босқичларида ҳисобатларни юритиш;

3. Ахборот хавфсизлиги инцидентларининг экспертизаси

Компютер инцидентларининг экспертизаси.

Бугунги кунда кичик ва ўрта бизнес корхоналари, банклар ва молия ташкилотлари, давлат бошқарув органлари ва бошқа ташкилотлар кибержиноятчиларнинг қурбони бўлиб қолмоқда ва кўрилган зарар миллионларни ташкил этмоқда, лекин энг муҳими оддий айланиб ўтишлар

амалга оширилганида эмас, балки, тизим фаолияти ва ҳимоясини баҳолаб, керакли ахборотларни йиғиб, ташкилот махфий маълумотларга рухсатни беркитиб кетишлари, келажакда бунданда кучлироқ инцидентларни ташкил этишларига ёлғочилишидир. Сир эмаски, кўплаб корхоналар бундай ҳолатларга қарши ҳеч қандай чора кўрмайди ва фақат зарарни қоплаш ҳақида бош қотиради, бу эса жиноятчиларга қўл келади.

IBM Security QRadar инцидентлар экспертизаси.

IBM Security QRadar инцидентлар экспертизаси экспертиза операцияларини ўтқазишда маълумотлар пакетини олиш ва бошқасида узатиш учун ишлатилади. Бу технология маълумотлар қидирув ишлари бошқаруви, сеансларни қайта қуриш ва инцидентлардан ҳимояланиш таҳлилини эксперт анализдан ўтказиш имконини беради. IBM Security QRadar инцидентлар экспертизаси воситалари дастурий ва аппарат кўринишида мавжуд.

ҚРадар дан самарали фойдаланиш учун дастлаб жуда кўп ёзувлар ичидан белгиланган ва келажакда эгалик учун қидирув ва белгилашларни киритиш лозим, бу бизга чекланган ёзувлар билан ишлаш имконини беради.

Таҳлилчилар ишни бошлаганда , уларнинг материаллари жуда кўп натижаларни қайтариши мумкин. Агар сиз ўзингизга нима керак эканлигини аниқ билмасангиз, маълум бир сўровни такрорлайверасиз ва бу элемент устида ҳеч қандай натижа бермайди.

Визуаллаштириш ва анализлар натижалар мослигини амалий ёки автоматик баҳолаш учун ишлатилиши мумкин. Бундан ташқари бошқа сўровлар ёрдамида айни муаммога бошқа тарафдан қараш имконини мавжуд

Қачонки сиз ўз таҳлилингиз бўйича керакли натжага эришсангиз, уни янада чуқурроқ ўрганиш ва якуний ечимни топиш ва уни қўллаш учун ушбу қисмни алоҳида ўрганиш имконига эгасиз. Сиз етарли деб ўйлаганингиздан кўпроқ материал киритиш лозим.

Таҳлил бўлимларида мавжуд релевант натижалар тўпламига эга бўлганингиздан сўнг сиз ўз изланишларингизни аниқ ё`налишга

тўғирлашингиз мумкин. Визуалиатсиая ва таҳлил элементлари ёрдамида ҳар бир қисмдаги натижаларни янада чуқурроқ ўрганишингиз мумкин. Ишга алоқадор барча ҳужжатларни ва якуний ечимларни сақлаб қўйишингиз мумкин. Агар язувлар муҳим ҳисобланмаси уларни ўчириб ташлаш мумкин. Изланишлар жараёнининг шу нуқтасида сиз турли маълумотлар ичидан фақат муҳимларини ажратиб оласиз ва сизда энг муҳин маълумотлар тўплами мавжуд бўлади. Ушбу маълумотлар чоп этилиши, экспорт қилиниши ёки қайта ишлаш учун жўнатилиши мумкин.

4. Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг техник қўлланиши

Ахборот хавфсизлиги инцидентларини аниқлашнинг техник воситалари ва тизимлари.

Ҳимоянинг турли техник воситаларид ҳодисалари хавф – хатарлар, уларнинг бузулиши, мавжуд АХБТ ҳақида муҳим ахборот беради. Янада кенгроқ мақсадларда, яъни тармоқ ҳужумларини аниқлаш ва зарарли ҳаракатларни аниқлашда ҳужумларни аниқлаш тизимлар (IDS), махсус маълумотларни тарқалиб кетмаслигини олдини олиш учун (DLP тизимлари) фойдаланилади, бошқача қилиб айтганда аппарат – дастурий воситалар тармоқ ҳолатини, ахборот оқимини, фоядаланувчилар ҳаракатларини назоратда ушлайди. Ахборот хавфсизлиги воситаларининг замонавий тенденсияси инцидентлар ҳақида ва Ахборот хавфсизлиги тизими ҳақида маълумотлар олиш учун тор доирадаги датурлардан кўра интеграллашган ва автоматлаштирилган дастурий аппарат воситалар, бир вақтда бир нечта вазифаларни бажарувчи Ахборот хавфсизлиги таъминотини талаб қилади.

Асосий вазифаларни Ахборот хавфсизлиги инцидентларини аниқлаш тизимлари техник воситалари ёрдамида ҳал қиламиз, булар:

- Умумий ҳодисалар манбаларидан ҳодисаларни қайта ишлаш орқали саралаш ва марказлашган маълумотларни йиғиш.
- Реал вақт режимида ҳужумларни, ЗД ларни ва Ахборот хавфсизлиги

сиёсати бузилишлари аниқлаш;

- Портлар орқали маълумотлар кириши ва чиқишини назорат қилиш;
- Фойдаланувчилар ҳаракатларининг миниторинги;
- Ахборот хавфсизлиги инцидентларини таҳлил қилиш учун барча далилларни тақдим этиш, уларнинг базаларини формаллаштириш;

Таҳлил олиб бориш учун маълумотларни йиғиш учун турли тизимлар иш журналлари, ҳодисалар ҳақида хабарлар, портлар ҳолатини кўриш, операцион тизим журналлари, иловалар, протоколлар, E-mail хабарлари ва бириктирилга файлларнинг қайсилари натижа учун зарур ва айни Ахборот хавфсизлиги инцидентни аниқлаш учун факт эканлигини излаш зарур.

Ахборот хавфсизлиги инцидентларига жавоб қайтаришда техник воситалар ва бошқа қўллаб – қуватлашлар.

Ахборот хавфсизлиги инцидентларига тезкор ва самарали жавоб қайтариш осон, қачонки барча зарур техник ва бошқа воситаларнинг қўллаб – қувватлашлари тайёрланганда, тестланганда ва айни ҳолатда олинганда. Бу чора – тадбирлар қуюдагича:

- ташкилот активлари ва бизнес функсияларига алоқадор маълумотларга руҳсат.
- мавжуд ва амалдаги режаларга ва бизнеснинг узлуксизлигини таъминловчи ҳужжатлаштирилган стратегияларга руҳсат.
- ахборот алмашинишдаги ҳужжатлаштирилган ва барчага маълум жараёнларга руҳсат.
- ахборот хавфсизлиги инцидентлари ва ҳодисалари элестрон МБ сидан ва МБ ни тўлдириш ва янгилаш учун техник воситалари, анализ натижалари ва жавоб қайтариш жараёнлари маълумотлари фойдаланиш(ташкилот томонидан фойдаланилган ва талаб этилган ёзувлар).
- резерв нусхаларни тестлаш.
- ЗД ларнинг назорати.
- тизим ахборотларининг айни ташувчилари ва ДТ лар.
- бизнес узлуксизлигини таъминлаш учун белгиланган режага мос тизим

ва дасурлар ишончли ва янгиланган версиялари.

Ҳужум уюштирилган ахборот тизимида, хизматлар ва тармоқ нотўғри ишлаши мумкин. Шунинг учун ташкилотда фойдаланилаётган техник қурилмалар иши (дастурий ёки дастурий – аппарат воситалар) ахборот хавфсизлиги инцидентларига жавоб қайтаришда зарур ва лекин фақат тармоққа, тизимга ва ёки сервисларга мўлжалланган бўлишига мажбур эмас. Ахборот хавфсизлиги инцидентларига жавоб қайтариш техник қурилмалари бутунлай автоном болиши ҳам мумкин.

Барча техник воситалар пухталик билан танланган, тўғри ўрнатилган ва тестланган (тестлашда барча натижаларда нусха олинади) бўлиши зарур.

Таъкидлаш жоизки, бўлимларга бириктирилган техник воситалар жавобгар шахс кузатувисиз автоматик тарзда ахборот хавфсизлиги инцидентларини ва ҳужумларни аниқлашни ва қўшимча ресурслар ва қурилмалар ишлатишни ўз ичига қамраб олмайди.

Фойдаланилган адабиётлар

1. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари

2. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар

3. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

4. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

7-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг ҳаёт даври процедураси

Режа:

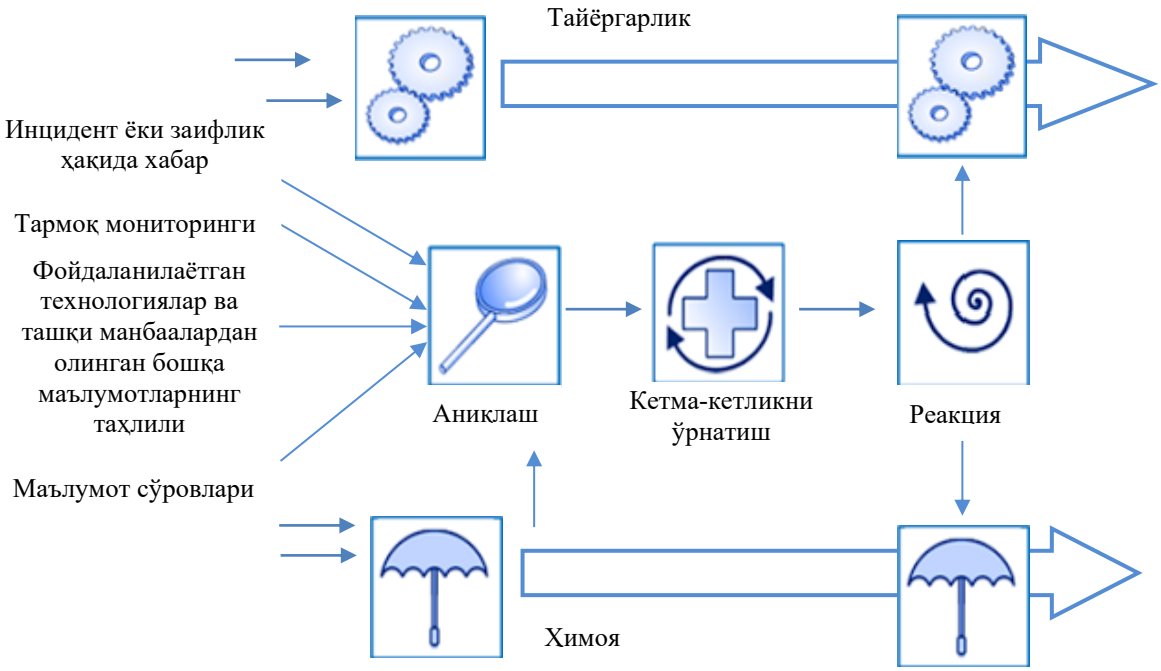
1. Инцидентларга жавоб қайтариш процедуралари (тартиби)
2. Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг зарурий процедуралари
3. Инцидентга жавоб қайтариш режасининг тузилиши
4. Инцидентга жавоб қайтаришни амалга ошириш принциплари
5. Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг техник ва бошқа томондан қўллаб-қувватланиши

1. Инцидентларга жавоб қайтариш процедуралари (тартиби)

Биз биламизки, компанияда инцидент юзага келган вақтда жамоалар ўзини қандай тутиши ҳақида олдиндан ишлаб чиқилган процедуралар бўлиши керак. Лекин бу қандай процедуралар? Гарчи, турли компаниялар бу процедураларни (ёки босқичларни) турлича талқин этсалар ҳам, лекин аслини олганда улар бир хил вазифани бажарадилар. Инцидентларга жавоб қайтариш – бу динамик жараён ҳисобланади. Унинг айрим босқичлари параллель ҳолда бажарилади, бошқалари эса кетма-кетликда, яъни кейинги босқич олдинги босқич натижаларига боғлиқ бўлган ҳолда бажарилади. Компания воқеа-ҳодисаларнинг тегишли ҳужжатлаштиришларини таъминлаб берувчи методик ёндашувдан фойдаланиши жуда муҳим бўлиб, бу эса инцидентларга жавоб қайтариш жараёнининг кейинги босқичларида ёки мабодо иш судгача борадиган бўлса, ва сиздан стандарт процедураларга риоя қилганмисиз, айрим қадамларни қолдириб кетмагансизми, деб сўраганларида муҳим аҳамият касб этади. Ўтказилган тадбирлар ва бажарилган ишлар ҳақидаги сизнинг қайдларингиз судда мақбул исбот бўлиб хизмат қилиши мумкин.

Инцидентларга жавоб қайтариш учун қуйидаги процедуралар тўпламини англаб етиш лозим:

- Кетма-кетликнинг ўрнатилиши;
- Локализация;
- Текшириш;
- Анализ;
- Кузатиш;
- Тиклаш.



6.1-расм. Инцидентларга жавоб қайтариш процедуралари

Инцидент оқибатлари тарқалишига қарши таъсир кўрсатиш стратегияси.

Инцидент тарқалишига қарши таъсир кўрсатиш процедураси – тартиби ҳар бир аниқ инцидент учун алоҳида қурилади ва унинг турига боғлиқ бўлади. Қарши таъсир кўрсатиш стратегиясининг мезонлари шакллантирилган бўлиши ва жавоб қайтариш жамоасининг барча иштирокчилари учун рухсат этилган бўлиши керак. Стратегияни аниқлашнинг мезонлари қуйидаги асосий позицияларни ўз ичига олади:

- активнинг потенциал шикастланиш (бузилиш) эҳтимоли ёки ўғирланиши;
- инцидент гувоҳномаларини сақлашга бўлган талаб;
- активга кириш мумкинлиги;

- қарши таъсир кўрсатишни амалга ошириш учун зарур бўлган вақт ва керакли ресурслар;
- қарши таъсир кўрсатиш стратегиясининг самарадорлиги (муаммонинг қисман ёки тўлиқ ҳал этилиши);
- стратегиянинг амал қилиш муддати (ҳафта, ой, чорак ва ҳ.).

Бир талай ҳолларда, ёвуз ниятли кимсани ўрганиш ва инцидентга керакли гувоҳномаларни тўплаш ҳолатларида четга олиб қўйилган (назорат қилинадиган) тўхтатиш стратегияси қўлланилади, бунинг моҳияти бузғунчи ҳатти-ҳаракатини аниқлаш, таҳлил қилиш, классификация қилиш – таснифлаш ва назорат қилиш (таъқиб қилиш)дан иборат бўлади. Ушбу методика юқори даражадаги самарадорлик билан бирга юқори даражадаги хавф-хатарга учраш эҳтимолига ҳам эга, модомики ёвуз ниятли кимса дискредитация (обрўсизлантириш) ресурси – усулидан ташкилотнинг бошқа активларига (фаолларига) ҳужум қилиш мақсадида фойдаланиши мумкин. Ташкилотда жавоб қайтариш жамоасининг юқори малакали экспертлари ва ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг ишлаб чиқилган сиёсати мавжуд бўлган шароитларда назорат қилинаётган тўхтатишнинг эҳтимоли мавжуд.

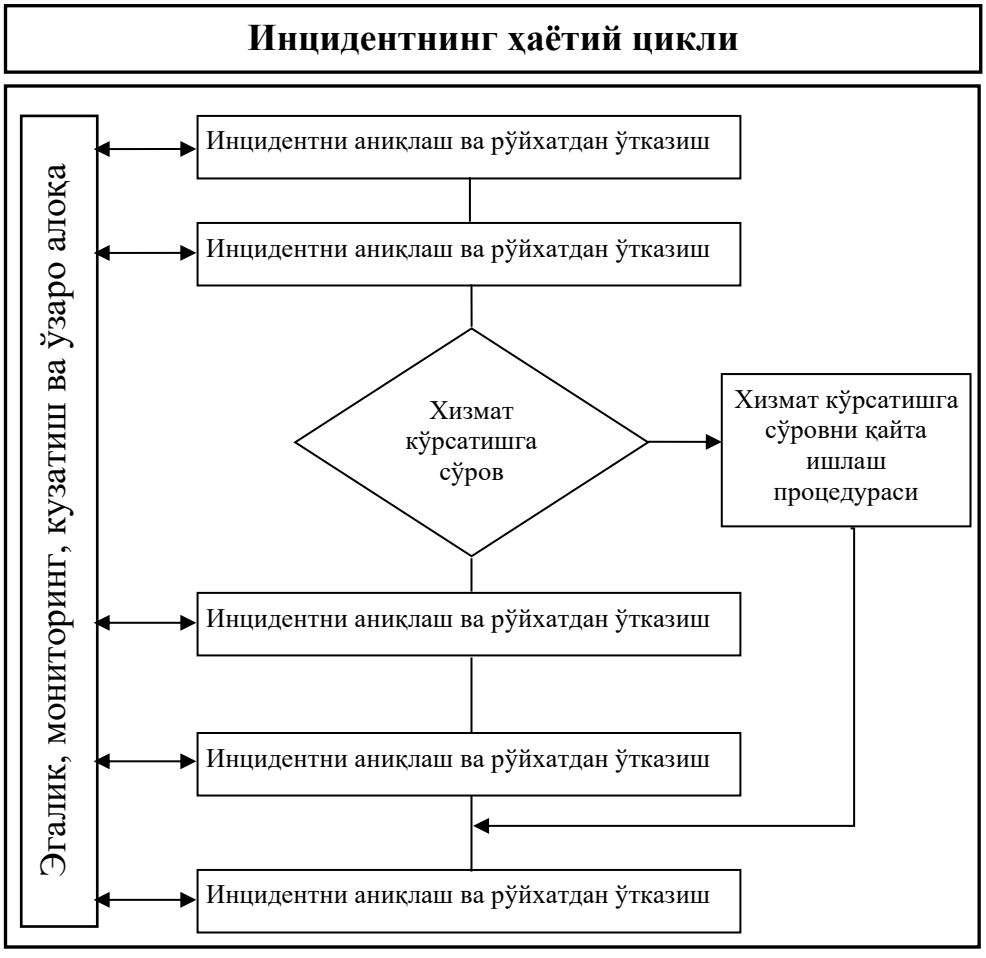
2. Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг зарурий процедуралари

Инцидентларга жавоб қайтариш процедураси бир неча даврдан иборат бўлиб, ходимларни ўқитиш ва зарур асбобларни тўплашдан бошланади ва инцидентдан чиққунча (текширишни тугатиш ва оқибатларни бартараф этгунча) давом этади. Ташкилот тайёрланиш жараёнида корреляция – ўзаро боғлиқлик тизимини тўғрилаб ва ташкилот ичи ва ташқарисида ахборотлар тарқалиши процедурасини синчиклаб ишлаб чиқиб, шубҳали ҳодисаларнинг потенциал сонини чегаралашга ҳаракат қилади. Тайёрланиш жараёнида ташкилот ахборот хавсизлиги хавф-хатарини баҳолайди. Инцидентларнинг ишлаб чиқиш жараёнини жиддий равишда енгиллаштирадиган энг яхши

амалиёт – бу Ахборот Хавфсизлиги Менеджмент Тизимини (АХМТ) жорий этишдир. Инцидентни текшириш ишлари қолган хавф-хатарларни баҳолаш процедураси ва келгуси ишлар учун амалий жиҳатдан фойда чиқариш билан якунланади.

Ёрдамчи жараёнлар структурасида молиявий ташкилотни бошқариш жараёнларини қўллаб қувватланишини таъминловчи ахборот хавфсизлиги инцидентларига жавоб қайтариш процедураларини қўллаш учун раҳбариятнинг қўллаб-қувватлашига мувофиқ равишда ахборот хавфсизлигини таъминлаш муаммосига ёндашувни қайта кўриб чиқиш талаб этилади.

Ахборот хавфсизлигини таъминлаш процедурасини жорий этиш механизмлари ташкилот жараёнлари тузилишида етарли даражада катта ҳажмли ҳисобланади.



6.2-расм. Инцидентнинг ҳаётий цикли

3. Инцидентга жавоб қайтариш режасининг тузилиши

Ташкилотни инцидентга жавоб қайтариш режасини шакллантириш, у билан таъминлаш ва уни мунтазам равишда тестдан ўтказиш муҳим аҳамият касб этади. Инцидентга жавоб қайтаришнинг яхши тузилган режаси нафақат хавфсизлик тизимини бузиб киришдан келадиган зарарни, балки жамиятнинг салбий фикр-мулоҳазаларини ҳам камайтиради.

Хавфсизлик жамоаси нуқтаи назаридан бу бузиб кириш қаердан бажарилганининг аҳамияти йўқ (одатда бу нарса очиқ тизим, масалан Интернет орқали амалга оширилади), энг аҳамиятлиси, у *қачон* содир бўлгани. Сизнинг тизимингиз заиф, унда дадиллик етишмайди деб бўлмайди; шуни тушуниб етиш муҳимки, етарли вақт ва ресурсларга эга бўлган ҳолда ҳаттоки энг қаттиқ ҳимояланадиган тизим ёки тармоқни ҳам бузиш мумкин.

Тизимни бузиш муқаррарлигини англаш ижобий натижага ҳам эга – бу эса хавфсизлик жамоасига потенциал зарарни камайтириш бўйича ҳаракатлар йўналишини танлаш имконини беради. Мавжуд тажрибага суянган ҳолда ва ушбу йўналишга амал қилган ҳолда жамоа фавқулоддаги ҳолатга тез ва ваҳимасиз жавоб қайтариши мумкин.

Инцидентга жавоб қайтариш режасини тўрт босқичга бўлиш мумкин:

- Воқеа-ҳодиса ривожини тўхтатувчи ёки секинлаштирувчи кечиктириб бўлмайдиган ҳаракатлар;
- Инцидентни текшириш;
- Тегилмаган, дахлсиз ресурсларни тиклаш;
- Мувофиқ каналлар бўйича инцидент ҳақида маълумот бериш.

Инцидентга реакция – жавоб аниқ ва тез бўлиши лозим. Амалий жиҳатдан хатоларга йўл қўйиб бўлмайди, шунинг учун бу режани амалиётда текшириб кўриш ва ҳаракатлар бажарилиш тезлигини ўлчаш муҳим аҳамиятга эга. Шунингдек, тезлик аниқлиги ва уни ошириш, ўзлаштириб бўлмайдиган зарарни камайтириш ва тизимнинг аниқ компрометацияси (обрўсизлантирилиши) методологиясини ишлаб чиқиш мумкин.

Инцидентга жавоб қайтариш режаси ўз ичига белгиланган талабларни киргизиши керак, жумладан:

- Компания экспертлари жамоаси (*Компьютер инцидентларига жавоб қайтариш жамоаси*);
- Ҳуқуқий жиҳатдан асосланган ва маъқулланган стратегия;
- Компаниянинг молиявий томондан қўллаб-қувватлаши;
- Раҳбариятнинг юқори даражадаги кўмаги;
- Тўғрилиги текширилган ва бажариладиган иш-ҳаракатлар режаси;
- Табиий ресурслар, масалан, маълумотлар базасини такрорлайдиган, компьютерларни ва заҳирадаги нусхалаш хизматини тайёр ҳолатга келтирадиган ресурслар.

4. Инцидентга жавоб қайтаришни амалга ошириш принциплари

Ташкилот бизнесини узлуксиз бошқариш лойиҳасини амалга ошириш перманент ҳаракатланувчи жараёнлар тўпламини ифодалайди: ташкилотнинг таҳлили, бизнес узлуксизлигини бошқариш стратегиясини қайтадан кўриб чиқиш, бизнес узлуксизлигини бошқариш процедурасини жорий этиш ва қайтадан баҳолаш, бизнес узлуксизлигини бошқаришга кўмаклашиш, яхшилаш ва аудит жараёни. Бизнес узлуксизлигини бошқариш процедурасини жорий этиш ҳолатини таҳлил қилишнинг асосий маълумотлар манбаларидан бири бўлиб, ахборот хавфсизлиги инцидентларига жавоб қайтариш процедураси ҳисобланади.

Жаҳон амалиётига мувофиқ айрим энг яхши принципларни шакллантирамиз, қайсики бу принципларга амал қилган ташкилот ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг самарали сиёсати билан таъминланади:

Ташкилот раҳбарияти ташкилот ичида ахборот хавфсизлиги инцидентларини текшириш процедурасини тадбиқ этиш учун зарур шарт-шароитларни туғдиришга имкон яратиши керак, чунончи:

- инцидентларга жавоб қайтаришнинг расмийлаштирилган сиёсатини яратиш;
- инцидентларни қайта ишлаш процедураларини ишлаб чиқиш;

- текшириш жараёнида маълумотларга мурожаат қилишда ҳуқуқий жиҳатларни тартибга солиш;
- инцидентларга жавоб қайтариш жамоа таркибини тасдиқлаш;
- инцидентлар тергови бўйича жамоанинг умумий мутахассислари (ҳуқуқшунослар, ходимлар, бизнесга кўмаклашувчи хизмат ходимлари, ахборот хавфсизлиги ва ҳ.) билан ташкилот ичидаги алоқаларини яхши йўлга қўйиш;
- тергов жамоасининг зоналарни белгилаш бўйича жавобгарлиги, текширув жамоасини ўқитиш ва техник жиҳатдан жиҳозлаш.

5. Ахборот хавфсизлиги инцидентларига жавоб қайтаришнинг техник ва бошқа томондан қўллаб-қувватланиши

Қачонки техник ва бошқа кўмаклашувчи зарур воситалар олинган, тайёрланган ва тестдан ўтказилган бўлса, АХ инцидентларига тез ва самарали жавоб қайтаришни амалга ошириш бир мунча осон бўлади. Бу чора-тадбирлар қуйидагиларни ўз ичига олади:

- ташкилот активлари деталлари – қисмларига (активларнинг янгиланган рўйхати мавжудлиги афзал) ва бизнес-вазифалар билан боғлиқ маълумотларга киришга рухсат этилади;
- бизнес узлуксизлиги таъминланишининг ҳужжатлаштирилган стратегияси ва унга мувофиқ режаларга киришга рухсат этилади;
- маълумотлар узатилишининг ҳужжатлаштириш ва босиб чиқарилиш жараёнлари;
- АХ инцидентлари воқеа-ҳодисалари тўғрисидаги маълумотлар базасини тезда тўлдириш ва янгилаш, жавоб қайтариш жараёнида маълумотларни таҳлил қилиш ва соддалаштириш учун маълумотларнинг электрон базаси ва техник воситалардан фойдаланиш (гарчи ҳамма тан олган бўлса ҳам, баъзан қўлда қайд этилган ёзувлар ҳам талабга жавоб беради ва ташкилот томонидан фойдаланилади);
- АХ инцидентлари воқеа-ҳодисалари тўғрисидаги маълумотлар базаси

учун бизнес узлуксизлигини таъминланишнинг адекват чора-тадбирлари.

АХ инцидентларига жавоб қайтариш жараёнини енгиллаштириш ва маълумотлар базаси ва ахборотлар мазмунини таҳлил қилишда, маълумотлар базасини тезда тўлдириш ва янгилашда фойдаланиладиган техник воситалар қуйидагиларга кўмаклашиши керак:

- АХ инцидентлари ва воқеа-ҳодисалари тўғрисида ҳисоботларни тезда олиш;
- бу воситалар (масалан, электрон манзил, факс, телефон орқали ва ҳ.) учун мос келадиган аввал танлаб олинган ходимларга (бунга тўғри келадиган бегона шахслар) хабар билдириш, яъни ишончли алоқалар маълумотлар базасидан ёрдам сўраган ҳолда (бу база ҳар доим кириш осон бўлиши ва ўз ичига қоғозли ҳужжатлар ва уларнинг нусхаларини киритган бўлиши керак) ва ахборотларни узатиш воситаси хавфсиз усулда (зарурат туғилганда) бўлиши лозим;
- Интернет ёки бошқа воситалар орқали амалга оширилган тизимга, сервис ва (ёки) тармоққа ҳужум қилинган вақтда электрон алоқани эшитишга йўл қўймаслик учун баҳоласа бўладиган хавф-хатарларга мувофиқ эҳтиёткорлик чораларига риоя қилиш;
- Интернет ёки бошқа воситалар орқали амалга оширилган тизимга, сервис ва (ёки) тармоққа ҳужум қилинган вақтда электрон алоқага киришни сақлаш учун баҳоласа бўладиган хавф-хатарларга мувофиқ эҳтиёткорлик чораларига риоя қилиш;
- ахборот тизими, сервис ва (ёки) тармоқлардаги ва барча ишлаб чиқилган маълумотларни тўплаш жараёни;
- ўзгаришлар мавжудлигини белгилашда кўмаклашиш учун ва ўша тизим, сервис ва (ёки) тармоқнинг баъзи қисмлари ва маълумотлар ўзгаришларга дуч келса, агар бу баҳоласа бўладиган хавф-хатарларга мос келса, яхлитликнинг криптографик назоратидан фойдаланиш;
- архивлаштириш ва тўпланган маълумотларни соддалаштириш (масалан, рўйхатга олиш журналидаги ёзувлар ёки бошқа маълумотномалар

ўрнига рақамли ёзувларни қўллаш ёки CD ёки DVD ROM мосламаларида фақат ўқиш учун мўлжалланган тарқатувчиларни автоном режимда сақлашдан олдин);

- АХ инцидентлари ривожланишини намойиш қилувчи, инцидент жараёнига рухсат этувчи ва ахборотлар сақланишини таъминловчи чопламаларга тайёргарлик (масалан, рўйхатга олиш журналлари);
- маълумотлар тизими, сервис ва (ёки) тармоқларнинг штатли иш тартибини қуйидагилар ёрдамида тиклаш:
- захирага олиб қўйишнинг оптимал – энг қулай процедураси,
- захирада турган аниқ ва ишончли нусхалар,
- захира нусхаларни тестдан ўтказиш, зарарли дастурларни назорат қилиш,
- тизимдаги ва амалий дастурий таъминотдаги бошланғич маълумотларни тарқатувчилар,
- бизнес узлуксизлигини таъминлаш режасига мувофиқ тизим ва иловалар учун келишилган ишончли ва янгиланган тузатишлар (“патчлар”).

Ҳужум қилинган ахборотлар тизими, сервис ва (ёки) тармоқ аниқ ишламаслиги мумкин. Шунинг учун, АХ инцидентларига жавоб қайтариш учун зарур бўлган техник воситалар иши (дастурий ёки аппарат таъминоти) ташкилотда фойдаланиладиган тизим, сервис ва (ёки) тармоқларга асосланган бўлмаслиги керак. Имкон борича, инцидентларига жавоб қайтарувчи техник воситалар тўлиқ автоном – мустақил бўлиши лозим.

Барча техник воситалар синчковлик билан танланган, тўғри жорий қилинган ва мунтазам равишда тестдан ўтказилган бўлиши керак (олинган резерв нусхаларни тестдан ўтказишни киритган ҳолда).

Шуни айтиб ўтиш керакки, йўқорида таърифланган техник воситалар, бевосита АХ инцидентларини ва рухсатсиз киришларни аниқлаш ва тегишли шахсларга автоматик равишда хабар беришда техник воситаларни ўз ичига олмайи.

Фойдаланилган адабиётлар

1. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари
2. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар
3. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.
4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

8-маъруза.

Мавзу: Ахборот хавфсизлиги интцидентларига жавоб қайтариш гуруҳи

Режа:

1. Ахборот хавсизлиги инцидентларига жавоб қайтариш
2. Ахборот хавфсизлиги инцидентларига жавоб қайтариш гуруҳи
3. Инцидентга мос роллар ва функциялар
4. Service Desk ходимларининг роли ва жавобгарликлари

1. Ахборот хавсизлиги ҳужумларига жавоб қайтариш

Бугунги кунда ахборот хавфсизлиги интцидентларига жавоб қайтариш (АХИЖҚ) долзарб муаммолардан ҳисобланади. Биринчидан, бу мавзу жуда оммабоп, бошқа томондан, у мавҳумлик муаммоси билан боғлиқ, чунки айнан текширув вақтида тизимнинг аниқ заиф томонлари, тахдидларнинг излари аниқланиб, АХ ходимларининг малакаси, АХ тизимининг тузилиш сифати текширилади.

Шуни таъкидлаб ўтиш жоизки, компанияда ахборот хавфсизлигига бўлган ҳужумлар яширилади, сабаби ҳеч ким ўз хатоларини тан олишни ҳоҳламайди ва шу билан рақобатчиларга қўшимча асослар беришни ҳоҳламайдилар. Бунинг натижасида ҳужумларнинг сони узлуксиз равишда ўсиб боради, улар тўғрисидаги маълумот эса қоида бўйича сир сақланади ва биз ОАВ да эълон қилинган кам миқдордаги ҳужумлар тўгрисидаги маълумотларгагина эга бўла оламиз. Бошқа томондан бундай “аниқлик” компютер ҳужумларини тавтиш этувчи мутахассисларни қидиришдаги ёки компаниянинг ҳужумларга жавоб қайтариш жараёнини ташкил этишдаги қийинчиликларни англатади. Умуман олганда, аниқ сабабларга кўра ижрочи ўз мижозларининг бажарилган иш тўғрисидаги мурожатларга жавоб қайтара олмайди. Шунингдек, бу турдаги ишларни бажариш ижрочи ва буюртмачи ўртасидаги ишончни талаб этади.

Бу турдаги мутахассисдан нималар талаб этилишини санаб ўтишга ҳаракат қиламиз:

- Хавфсизлик принсипларини англаш;
- Ахборот объектларининг нуқсонлари ва заифликларини билиш;
- Интернет қурилмалари ҳақида тушунча;
- Ахборот тизимига қарши хавф-хатарлар таҳлили бўйича кўникма;
- Тармоқ протоколларини билиш;
- Тармоқ иловалари ва сервис ҳақида билиш;
- Тармоқ хавфсизлиги муаммоларини билиш;
- Тугун ёки тизим хавфсизлиги муаммолари ҳақида тушунча;
- Зараркунанда дастурлар (вирус, троянлар) тўғрисида тушунча;
- Дастурлаш малакасига эга бўлиш.

2. Ахборот хавфсизлиги инцидентларига жавоб қайтариш гуруҳи

Ахборот хавфсизлиги интцидентларига жавоб қайтариш гуруҳи (ing. Information Security Incident Response Team (АХИЖҚГ)) бу ташкилотнинг ишончли ва малакали аъзолари гуруҳи бўлиб, ахборот тизимларига тегишли белгиланган жавобгарлик доирасида ахборот хавфсизлигининг бузилишига жавоб қайтаришни бажаради, координатсиялайди ва жараённи ушлаб туради.

АХИЖҚГ ни яратишдан мақсад ахборотни юбориш жараёни ва қайта алоқа, бошқариш, керакли координатсия кабилардан дарс олиш, бундан ташқари АХ Инцидентларига жавоб қайтариш, баҳолаш учун ташкилотни мос персонал билан таъминлашдан иборат. АХИЖҚГ аъзолари АХ ҳужумларига боғлиқ бўлган жисмоний ва молиявий зарарни шунингдек, корхонанинг номини тиклашдаги зарарни камайтиришда қатнашишлари мумкин.

АХИЖҚГ таркиби миқдор, йўналиш, ташкилий-ҳуқуқий тузилма ва бошқа компания бошқарувининг характеристикаларига боғлиқ. Шунингдек, АХИЖҚГ нинг минимал таркиби: АХИЖҚГ бошарувчиси, регистратор-баҳоловчи, ҳужумлар регистратсияси МБ администратори, компютер суд экспертизаси мутаҳҳассиси, юрист, тизим масалалари бўйича мутахассис, тармоқ масалалари бўйича мутахассис ва ахборот хавфсизлиги бўйича мутахассис-експерт.

АХИЖҚГ изолятсияланган гуруҳ бўлиб, персоналининг асосий вазифаси ҳужумларни тавтиш қилиш ҳисобланмайди, регитратор-баҳоловчи ва ҳужумлар регистратсияси МБ администратор бундан мустасно. Ахборот хавфсизлигига ҳужумнинг турига қараб АХИЖҚГ аъзолигига шартнома асосида аниқ ихтисослашган масалалар бўйича мутахассислар олиниши мумкин. Гуруҳ азолари ички лавозим вазифаларидан келиб чиққан ҳолда АХИЖҚГ ичида бир қанча функцияларни бажариши мумкин.

Еслатмалар

Берилган группа ташқи экспертлар билан тўлдирилиши мумкин масалан, тан олинган жавоб қайтариш гуруҳидан компютер ҳужумлари ёки тезкор жавоб қайтариш гуруҳига.

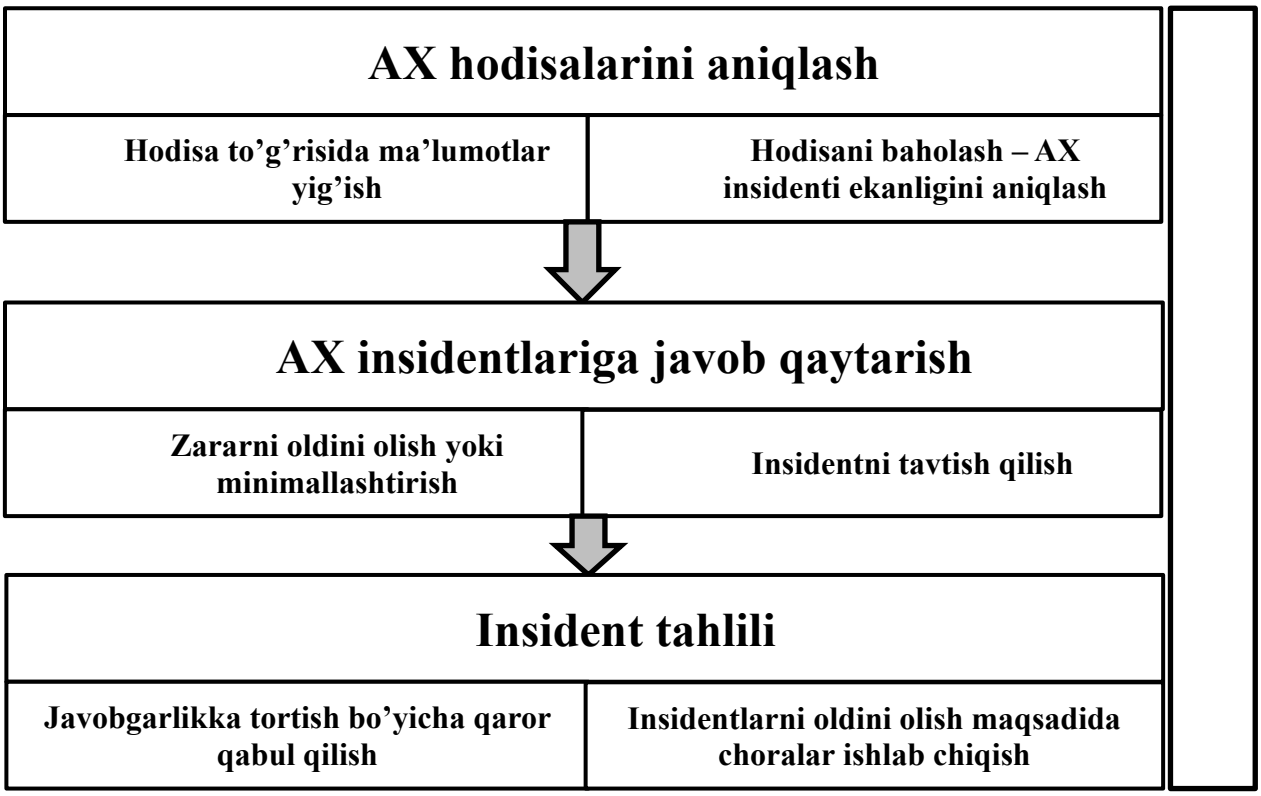
АХИЖҚГ ни яратишдан мақсад ахборотни юбориш жараёни ва қайта алоқа, бошқариш, керакли координатсия кабилардан дарс олиш, бундан ташқари АХ Инцидентларига жавоб қайтариш, баҳолаш учун ташкилотни мос персонал билан таъминлашдан иборат. АХИЖҚГ аъзолари АХ ҳужумларига боғлиқ бўлган жисмоний ва молиявий зарарни шунингдек, корхонанинг номини тиклашдаги зарарни камайтиришда қатнашишлари мумкин.

АХИЖҚГ таркиби

Ушбу персоналнинг миқдор ва таркиби ташкилот фаолияти мақсади ва масштабига мос тушиши лозим.

АХИЖҚГ алоҳида тузилган гуруҳ ёки корхонанинг турли бўлимларидан (масалан, ахборот технологиялари / телекоммуникатсиялари, бухгалтерия, кадрлар бўлими ва маркетинг) жалб этилган ходимлар жамоаси бўлиши мумкин.

АХИЖҚГ бошқарув аъзоларини хабардор қилиш учун бошқа бизнес жараёнларидан алоҳида бўлган тизимга эга бўлиши керак.



8.1-расм. АХ инцидентларига жавоб қайтариш гуруҳининг ишлаш жараёни

АХИЖҚГ мажбуриятлари

АХИЖҚГ мажбуриятларини 2та асосий гуруҳга ажратиш мумкин:

- ***Жорий вақтдаги ҳаракатлар,*** асосий масала билан боғлиқ – таҳдидларга жавоб қайтариш;
- ***Профилактик ҳаракатлат,*** жорий вақт масштабида юзага келмайдиган ва ёрдамлашувчи вазифани бажарадиган ҳаракатлар.

Биринчи гуруҳ кирувчи ҳисоботларни (ҳужумлар классификатсияси) баҳолаш ва бошқа ташкилотлар(жавоб қайтариш кординатсияси), гуруҳлар ва интернет хизматлари таъминотчилари билан биргаликда қабул қилинган маълумотлар устида иш олиб бориш, шунингдек, ҳужумдан сўнг ишни тиклашда(муаммоларни ҳал қилиш) локал фойдаланувчиларга ёрдам беришни ўз ичига олади.

Ҳужумлар классификатсияси қуйидагиларни ўз ичига олади:

- ***ҳисоботларни баҳолаш:*** кирувчи маълумот муҳимлилик даражасига қараб тартибланади, бунда давом этаётган ҳодисалар ва аниқланган тенденсияларга боғлиқ бўлади.

- ***текширув:*** ҳужум ва унинг масштаби аниқланади

Жавоб қайтариш кординатсияси ўз ичига қуйидагиларни олади:

- ***ахборотни категориялаш:*** ҳужумга тааллуқли бўлган маълумот (рўйхатга олиш журналлари, боғланиш маълумотлари ва ҳк) ахборотларни ошкор қилиш сиёсатига асосланган ҳолда категорияланади.
- ***кординатсия:*** ахборотларни ошкор қилиш сиёсатига кўра бошқалар ҳужум ҳақида хабардор этиладилар.

Муаммоларни бартараф этишнинг вазифалари қуйидагилар:

- ***техник таъминот;***
- ***муаммоларни ҳал этиш:*** ҳужум ва унинг пайдо бўлиш сабабларини йўқотиш;
- ***қайта тиклаш:*** тизимни нормал ҳолатга қайтаришда ёрдам кўрсатиш.

Профилактик ҳаракатларга қуйидагилар киради:

Маълумотлар билан таъминлаш: маълум заиф жойлар, олдинги муаммолар ечиш йўллари ёки консултатсия мақсадида ҳаволалар рўйҳатини ташкил этиш; хавфсизлик воситаларини тақдим этиш (масалан, аудит воситалари).

- кадрларни ўқитиш ва тайёрлаш;
- маҳсулотларни баҳолаш;
- ташкилотнинг ҳимояланганлилигини баҳолаш;
- консултатсия хизматлари.

3. Инцидентга мос роллар ва функциялар

Жараёнларнинг реализатсияси горизонтал йўналишда ташкилотнинг иерархик структураси орқали олиб борилади. Бу фақатгина жараёнларнинг реализатсиясига боғлиқ бўлган жавобгарлик ва ваколатларни аниқлашда юзага келади. Мослашувчанликни ошириш мақсадида ролли ёндшувдан фойдаланиш мумкин (ролларни аниқлаш). Катта бўлмаган ташкилотларда ёки умумий ҳаражатларни камайтириш мақсадида ролларни бирлаштириш мумкин, масалан, ўзгаришларни бошқариш ва конфигуратсияларни бошқариш

жараёнлари бошқарувчиси ролларини мослаштириш.

Ҳужумларни бошқариш жараёни бошқарувчиси

Кўплаб ташкилотларда ҳужумларни бошқариш бошқарувчиси ролини Service Desk хизмати менежери амалга оширади. Ҳужумларни бошқариш жараёни бошқарувчиси жавобгарлиги соҳасига қуйидагилар киради:

- жараённинг самарали ва ратсионал иши мониторинг;
- қўллаб қувватлаш гуруҳи ишини назорат қилиш;
- жараённинг боришини янада мукаммаллаштириш бўйича кўрсатмалар тузиш;
- ҳужумларни бошқариш тизимини ривожлантириш ва кузатиб бооpиш.

Қўллаб-қувватлаш гуруҳи персонали.

- Қўллаб қувватлашнинг 1-қисми рўйхатга олиш, классификатсия, таққослаш(ечим), қўллаб қувватлаш гуруҳига тарқатиш, ҳужумларни бартараф этиш ва ёпиш.
- Қолган қўллаб қувватлаш гуруҳлари тавтишда, диагностикада ва ҳужумларни бартараф этишда ўрнатилган ваколатлар доирасида қатнашадилар.

4. Service Desk ходимларининг роли ва жавобгарликлари

Service Desk – бу мижоз ёки фойдаланувчилар билан келишилган ҳолда тақдим этиладиган сервислар юзасидан жавобгар бўлган диспетчерлик хизмати эмас, барча талаб ва таклифларни қабул қилиш маркази, жорий сервизларнинг ҳолатини назорат қилувчи ва мавжуд ишдаги бузилишларни бартараф этиш учун нарядлар чиқариш ҳуқуқига эга, шунингдек, бузулишларни бартараф этиш жараёни устида назоратчи ҳисобланади.

Қўллаб қувватлаш ҳодимлари жавобгарликларини ажратишда ташкилотнинг ўлчами ва Service Desk ва бизнес ўртасидаги хизмат кўрсатиш даражасининг асосий шартларини ҳисобга олиш лозим. Шуни ёдда тутиш лозимки, гап мавқеларни эмас ролларни тарифлаш ҳақида кетяпти. Хизмат масалаларини ечиш учун қуйидаги ролларни ажратиб олиш керак:

- Қўллаб қувватлаш хизмати менежери;
- Қўллаб қувватлаш хизмати аналитиги.

1. Менежер.

Service Desk менежерининг асосий вазифалари бутун хизмат ишининг кординатсияси ва унинг узликсиз ривожланиши билан боғлиқ. Унинг асосий вазифалари қуйида кўрсатилган:

- хизмат аналитиклар ва кундалик жараёнларни бошқариш, ишни баҳолаш;
- иш самарадорлигининг мониторинг ва уни янада ривожлантириш бўйича тавсиялар тузиш;
- ходимларни тайёрлаш бўйича режаларини тузиш ва амалага ошириш;
- бошқарув ҳисобини ишлаб чиқиш;
- хизмат доирасида фойдаланиладиган жараёнларни амалга ошириш ва янгиларни ривожлантириш;
- хизмат ичида хизмат кўрсатиш маданиятини шакллантириш.

2. Аналитик (муҳандис, диспетчер).

Service Desk аналитигининг роли хизматнинг кундалик масалалари ва жараёнларини амалга ошириш бўйича жавобгарликдир. Бу рол, аввалambор, Ҳужумларни Бошқариш жараёнини амалга ошириш билан боғлиқ. Ҳужум ҳаёт сиклининг бошланғич даврида Service Desk аналитиклари ҳужумнинг аниқ регистратсия ва кллассификатсияси, бошланғич ёрдам кўрсатишга жавобгардирлар. Бошланғич ёрдам кўрсатиш босқичида белгиланган вақтинчалик чегаралар доирасида максимал миқдордаги ҳужумларни ҳал этишга жавобгардирлар. Бу ҳаракатлар тўғридан тўғри мижозни қониқтириш билан боғлиқ ва ёрдам кўрсатиш занжирида ҳужумнинг аниқлигини белгилайди. Хизмат аналитиклари дарҳол ҳал этилмаган ҳужумларни ҳисобга олишга жавобгарлар. Бу билан уларнинг жавобгарликлари тугаб қолмайди, улар хизмат кўрсатиш мақсадларига мос ҳолда уларни қайта ишланишини давом этаётганига кафолат бериш мақсадида ҳужум учун жавобгарликни сақлаб қоладилар. Шунингдек, у мижозга ҳужумнинг бутун ҳаёт сикли

давомида олиб борилаётган ишлар ҳақида маълумот бериб боради. Ҳужум ҳал этилиши билан аналитик мижознинг ечимдан кўнгли тўлганлигига амин бўлиш лозим ва шундан кейингина ҳужумни ёпиши мумкин. Бу рол шунингдек, Service Desk га келиб тушадиган барча турдаги сўровларни бошланғич қайта ишланишини ва Service Desk инфратузилмасининг knowледге басе (билимлар базаси) базаси ёки кўплаб бериладиган саволлар рўйхатини тўлдириб борилиши каби ички элементларини бажаришни ўз ичига олади. Бу рол қуйидаги ҳаракатлар учун жавобгардир:

Ҳужумни рўйхатга олиш

- бошланғич ёрдам кўрсатиш жараёнида ҳал этилмаган ҳужумларни ҳал этиш гуруҳига йўналтириш;
- бошланғич ёрдам кўрсатиш ва классификатсия;
- барча очиқ ҳужумларни ҳал этишдаги силжишлар ва статусни назорат қилиш;
- сўровлардаги силжишлар тўғрисида фойдаланувчиларни хабардор қилиш;
- лозим бўлганда ҳужум эскалатсиясини амалга ошириш.

Аналитикнинг асосий сифати доимий стресс ҳолатида ишлашга қодир бўлиш “зарбани қабул қилиш”ни билиш, масалаларни ечишда конструктив ёндашиш, шикоят ва айбловларга аниқ жавоб бериш ҳисобланади. Бу ассептивлик (қабулқилувчанлик) дейилади –қатъият бутун “негатив” оқимидан фойдали ахборотни ажратиб олиш хусусияти, ўша ахборотдан негативни юракка яқин олмаган ҳолда фойдаланиш.

Иккинчи зарур бўлган сифат – бу жамоада ишлай олиш қобилияти. “Юлдузлар” эмас, биргаликда ишлай оладиган одамлар керак.

Учинчи муҳим шахсий сифатлардан бири масъулиятлилик ҳисобланади, бу иш бўйича боғлиқ бўлган одамларда унинг ўз вақтида келиб, ўзининг иши билан машғул бўлиши тўғрисида ишонч мавжуд бўлиши учун керакдир.

Тўртинчи сифат – билимдонлик, катта миқдордаги маҳсулотлар тўғрисида маълумотлар ола билиш ва энг муҳими уни бажариш хоҳишининг

мавжудлиги, унда кенг аммо ахборот технологияларининг барча соҳаси бўйича чуқур бўлмаган билими бўлиши лозим. Кўп бериладиган саволар бўйича тушунчага эга бўлиш ва консултатсия олиш мумкин бўлган иккинчи босқичдаги мутахассислар гуруҳини билиши лозим.

Фойдаланилган адабиётлар

1. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари
2. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар
3. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.
4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

9-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларини бошқариш дастурлари

Режа:

1. Ахборот хавфсизлиги инцидентларини бошқариш дастурлари ва уларнинг вазифалари
2. Техник ва бошқа ёрдам (шу жумладан операцион ёрдам)
3. Бошқариш схемасини тестдан ўтказиш
4. Ахборот хавфсизлиги инцидентларини бошқариш дастурларига амалга ошириладиган ҳужумлар

1. Ахборот хавфсизлиги инцидентларини бошқариш дастурлари ва уларнинг вазифалари

Ахборот хавфсизлиги инцидентларини бошқариш дастурларининг асосий вазифаси АХИ ҳужжатларни тўлиқ яратилиш, АХИ қайта ишлаш жараёни ва кетма-кетлигини тавсифлаб бериши ҳвмда АХИ ҳақида хабардор этиш вазифаларини бажариши карак. Ахборот хавфсизлиги инцидентларини бошқариш дастурлари АХИ ҳодисаларига тегишли ҳаракатларини аниқлаши керак бўлади. Ахборот хавфсизлиги инцидентларини бошқариш дастурларининг қўлланилиши:

- ахборот хавфсизлиги инцидентларига жавоб қайтариш;
- инцидент аниқланиши, ниқланган инцидентни бартараф этиш ёки АХИ сфатида қабўл қилиши;
- ахборот хавфсизлиги инцидентларини рехсат берилгунча бошқариш;
- идентификация қилиниб аниқланган инцидентларини қайта ишлаш, ҳар эҳтимолга қарши хавфсизлик тизимини такомиллаштириш;
- идентификациялашни амалга оширишни яхшилаш.

Ахборот хавфсизлиги инцидентни таҳлиллашни аппарат ва дастурий таъминоти:

- компютер жиноятчилиги иш станциялари ёки захира қурилмалар, ноутбуклар;

- махсус (сервер иш станциялари ва тармоқ) қурилмалар;
- бўш маълумот ташувчи қурилмалар, кабеллар, бинолар, ўзгартгичлар ва ёзиш ҳуқуқини чеклаш;
- кичгина принтер;
- тармоқ протоколи ва пакетларни снифферлаш таҳлиллагичлари;
- компютер жиноятчилигини дастурий таминоти;
- маълумот сақловчи қурилмалар;
- далилларни йиғишдаги (мисол, ноутбуклар, камералар, ёзиб олувчи қурилмалар, далиллар йиғилган файллар папкаси) рухсатлар.

2. Техник ва бошқа ёрдам (шу жумладан операцион ёрдам)

Ахборот хавфсизлиги инцидентларига тез ва самарали жавоб берилишини таъминлаш учун ташкилот керакли техник ва бошқа ёрдам воситаларини сотиб олиши, тайёрлаши ва текшириши лозим. Буларга қуйидагилар киради:

a) ташкилот активларининг тавсифи, шу жумладан, активларнинг янгиланган руйхати ва уларнинг бизнес-функциялар билан алоқалари ҳақидаги маълумотлардан фойдаланиш имкони;

b) кризисга қарши бошқариш билан боғлиқ ҳужжатлаштирилган процедураларни ишлатиш имконияти;

c) ахборот узатишнинг ҳужжатлаштирилган ва эълон қилинган жараёнлари;

d) ахборот хавфсизлиги ҳодисалари/инцидентлари/заифликлари маълумотлар омборини ва техник воситаларни маълумотлар омборини тез тўлдириш ва янгилаш, ундаги ахборотни таҳлил қилиш ва жавоб бериш жараёнларини соддалаштириш учун қўллаш (айрим холларда ташкилотга қўлда қилинган ёзувлар керак бўлиши мумкин); маълумотлар омборини ишончли сақлаш;

e) ахборот хавфсизлиги эксперт далилларини йиғиш ва таҳлил қилиш учун ускуналар;

f) ахборот хавфсизлиги заифликлари ҳодисалари/инцидентлари/ заифликлари маълумотлар омборини кризисга қарши бошқаришнинг мутаносиб чоралари.

Ташкилот маълумотлар омборини тез киритиш ва янгилаш учун ишлатиладиган техник воситалар томонидан ахборотни таҳлил қилиш ва ахборот хавфсизлиги инцидентларига жавоб жараёнини енгиллаштиришни ҳамда уларнинг қуйидагиларда ёрдам беришини таъминлаш лозим:

a) ахборот хавфсизлиги ҳодисалари/инцидентлари/заифликлари ҳақидаги ҳисоботларни тез олиш;

b) тегишли олдиндан танланган учинчи шахсларнинг бу мақсад учун танланган воситалар (масалан, электрон почта, факс ва телефон) орқали ҳисобот бериши, яъни қулай ва қоғоздаги ва бошқа нусҳаларни ўз ичига олган ҳамда маълумотни хавфсиз усул билан (зарурат бўлганда) узатиш имкониятларига эга бўлган ишончли контакт маълумотлар омборининг ёрдамини сўраш орқали;

c) тизим, хизмат ва/ёки тармоққа ҳужум пайтида Интернет ёки бошқа восита орқали жорий қилинадиган электрон алоқанинг ишлашини таъминлайдиган, баҳоланган таҳдидларга мос эҳтиёт чораларининг кўрилиши (бунинг учун олдиндан тайёрланган муқобил алоқа воситаларини қўллаш керак бўлиши мумкин);

d) ахборот тизими, хизмати ва/ёки тармоғи ҳамда барча қайта ишланаётган маълумотлар ҳақидаги барча маълумотларни йиғиш жараёни;

e) ўзгаришлар мавжудлигини ҳамда тизим, хизмат ва/ёки тармоқнинг қайси қисмлари ва қайси маълумотлар ўзгартирилганини аниқлашга ёрдам бериш мақсадида бутунликни криптографик назорат қилиш усулини ишлатиш, агар бу баҳоланган таҳдидларга мос келса;

f) йиғилган ахборотни архивлаш ва ҳимоя қилишни соддалаштириш (масалан, фақат CD ёки DVD ROM қурилмаларида ўқиш учун мўлжалланган ташувчиларга автоном равишда сақлашдан олдин қайд журналларида рақамли имзо ёки бошқа ёзувларни қўллаш орқали);

g) ахборот хавфсизлиги инцидентини бартараф қилиш жараёнини акс эттирувчи ва ахборотнинг бутунлигини таъминловчи ҳужжатларни (масалан, қайд журналларини) чоп этишга тайёрлаш;

h) кризисга қарши бошқаришга мувофиқ равишда қуйидаги процедуралар орқали ахборот тизими, хизмати ва/ёки тармоғининг одатий иш режимини тиклаш:

- резерв нусҳаларини синовдан ўтказиш;
- зарарли дастурларни назорат қилиш;
- тизимли ва амалий дастурий таъминотга эга асл ахборот ташувчиларидан фойдаланиш;
- юкловчи ахборот ташувчиларни қўллаш;
- тизимли дастурий таъминот ва иловаларнинг тоза, ишончли янгиланишларини қўллаш.

Ташкилотлар орасида ўрнатувчи дискдан стандарт базавий образ яратиш ва бу образни тизим яратишнинг тоза асоси сифатида қўллаш кенг тарқалмоқда. Бундай образнинг оригинал манбаа ўрнига ишлатилиши кўпинча мақсадга мувофиқ, чунки образ ўзгартирилган, тасдиқланган, синалган ва ҳоказо.

Ҳужумга учраган ахборот тизими, хизмати ва/ёки тармоғи нотўғри фаолият кўрсатиши мумкин. Шунинг учун ахборот хавфсизлиги инцидентига жавоб бериш учун керакли техник воситаларнинг (дастурий ёки аппарат таъминоти) иши ташкилотда ишлатиладиган тизимлар, хизматлар ва/ёки тармоқларга асосланмаслиги лозим. Иложи борича ҳодисага жавоб беришнинг техник воситалари тўлиқ автоном бўлиши керак.

Изоҳ - Ушбу пункда кўрсатилган техник воситаларга бевосита ахборот хавфсизлиги инцидентлари ва хужумларини аниқлаш, шунингдек, тегишли шахсларни автоматик огоҳ қилишда ишлатилдагиган техник воситалар кирмайди.

Контакт посизияси (КП) ташкилотнинг ахборот технологиялари ва тегишли ахборотни қайта ишлаш билан боғлиқ барча аспектларини қўллаб-

қувватлашда кенг қамровда қўлланилса ҳам, ахборот хавфсизлиги инцидентларини бошқаришда муҳим рол ўйнайди. Агар ахборот хавфсизлиги воқеалари ҳақида биринчи марта хабар берилаётган бўлса, КП улар билан аниқлаш ва ҳисобот босқичида кўришади. КПда йиғилган маълумотни қайта кўриб чиқиш ва ҳодисани инцидент сифатида таснифлаш лозимлигига дастлабки баҳо бериш лозим. Агар ҳодиса инцидент сифатида таснифланадиган бўлса, КП у билан курашади, лекин аксар холларда инцидентни бартараф қилишга ахборот хавфсизлиги инцидентларига таъсир этиш хизмати масъул бўлиши лозим. КП ходимлари хавфсизлик бўйича экспертлар бўлишлари мақсадга мувофиқ.

3. Бошқариш схемасини тестдан ўтказиш

Ахборот хавфсизлиги ҳодисалари ва инцидентларини бошқариш жараёнида юзага келиши мумкин бўлган эҳтимолий камчиликлар ва муаммоларнинг олдини олиш учун ташкилот ахборот хавфсизлиги инцидентларини бошқариш жараёнлари ва процедураларини мунтазам текшириш ва назоратдан ўтказишни режалаштириши лозим. Ахборот хавфсизлиги инцидентига жавобни таҳлил қилиш натижасида юзага келадиган ҳар қандай ўзгаришлар жиддий текширув на назоратдан ўтиши лозим. Ташкилот тест процедураларининг таҳлили натижасида киритилган ҳар қандай ўзгаришларнинг батафсил текширилишини, шунингдек, ўзгарган бошқариш схемаси ишга тушишидан олдин кейинги текширувни кафолатлаши лозим.

4. Ахборот хавфсизлиги инцидентларини бошқариш дастурларига амалга ошириладиган ҳужумлар

1. Хизмат кўрсатишда рад этиш

Хизмат кўрсатишда рад этиш (DoS) ва хизмат кўрсатишда тақсимланган рад этиш (DDoS) - умумий йўналишга эга бўлган инцидентларнинг йирик категориялари. Бундай инцидентлар тизим, хизмат ёки тармоқнинг иши унинг имкониятлари тўлиқ ҳажмида тўхтаб қолишига сабаб бўлади ва одатда

муаллифлашган фойдаланувчиларнинг ҳам хизматдан фойдаланишини тўлиқ рад қилади. Техник воситалар билан боғлиқ DoS/DDoS инцидентларининг икки асосий тури мавжуд: манбаанинг йўқ қилиниши ва манбаанинг осилиб қолиши.

Атайлаб уюштирилган DoS/DDoS техник инцидентларининг айрим типик намуналари:

- тармоқ диапазонини жавоб трафики билан тўлдириш мақсадида тармоқ узатишини пинг-сўровлар ёрдамида текшириш;
- тизим, хизмат ёки тармоқни барбод қилиш ёки унинг нормал ишлашини тўхтатиш мақсадида унга номаълум форматда маълумотлар юбориш;
- конкрет тизим, хизмат ёки тармоқнинг ресурсларини тугатиш (яъни секинлаштириш, ёқиш ёки уларни ишлатишни рад этиш) мақсадида у билан рухсат этилган сессиялар тармоғини очиш.

Бундай ҳужумлар кўпинча бот-тармоқлар - автоном ва автоматик бошқариладиган дастурий роботлар (зарарли кодлар) орқали амалга оширилади. Бот-тармоқлар юзлаб, миллионлаб зарарланган компьютерларга алоқадор бўлиши мумкин.

Айрим техник DoS инцидентлари тасодифан, масалан, операторнинг нотўғри конфигурацияси ёки дастурий таъминотнинг мос келмаслиги туфайли юзага келган бўлиши мумкин, лекин аксар ҳолларда улар атайлаб уюштирилган бўлади. Айрим техник DoS инцидентлари атайлаб тизим ёки хизматни барбод қилиш, тармоқни ёпиш мақсадида уюштирилади, бошқалари эса бошқа зарарли фаолиятнинг натижаси бўлиши мумкин. Масалан, айрим идентификация ва сканерлаш усуллари сканерлаш пайтида эски тизимлар ёки нотўғри конфигурацияли тизимларнинг барбод бўлишига олиб келиши мумкин. Шуни қайд этиш лозимки, кўпинча техник DoS инцидентлари аноним тарзда ишга туширилади (яъни ҳужум манбаи соҳталаштирилган бўлади).

Техник воситалар сабабли юзага келган ва ахборот, хизмат ва/ёки воситаларнинг йўқотилиши билан тугайдиган DoS инцидентларига қуйидагилар мисол бўла олади:

- қурилманинг ўғирланиши, унга атайлаб зарар етказилиши ёки унинг ишдан чиқарилиши билан тугайдиган жисмоний хавфсизлик чораларининг бузилиши;
- ёнғин ёки сув тошқини натижасида аппарат воситалари (ва/ёки улар жойлашган жой)га тасодифан зарар етиши;
- атроф муҳитнинг фавқулодда ҳолатлари, масалан, иш шароитининг юқори ҳарорати (кондиционернинг ишдан чиқиши натижасида);
- системадаги узилишлар ёки ўчириб қайта ёқишлар;
- тизимнинг назорат қилинмаган ўзгаришлари;
- дастурий таъминот ёки аппарат воситаларидаги узилишлар.

2. Рухсатсиз фойдаланиш

Умуман олганда, инцидентларнинг бу гуруҳи тизим, хизмат ёки тармоқдан рухсатсиз фойдаланишга уринишдан иборат. Техник рухсатсиз фойдаланиш инцидентларига айрим мисоллар:

- пароллар файлларини тиклашга уриниш;
- объектдан тўлиқ (масалан, тармоқ маъмури даражасида) фойдалана олиш имкониятини қўлга киритиш учун алмашинув буферини тўлдириш ҳужуми;
- ресурслар ёки маълумотга фойдаланувчи ёки администратор қонуний асосларда эга бўлган фойдаланиш имкониятидан кўра кўпроқ даражада фойдаланиш имконини қўлга киритишга уринишлар.

Техник бўлмаган воситалар ёрдамида маълумотни бевосита ёки билвосита ошкор қилиш ёки ўзгартириш, бўйсунишнинг бузилиши ёки ахборот тизимларини нотўғри ишлатиш натижасида юзага келган рухсатсиз фойдаланиш инцидентларига қуйидагилар сабаб бўлиши мумкин:

- ахборотдан рухсатсиз фойдаланиш натижасида жисмоний хавфсизлик чораларининг бузилиши;
- тизимдаги назорат қилинмаган ўзгаришлар ёки дастурий ёки аппарат таъминотидаги узилишлар натижасида операцион тизимнинг ёмон ва/ёки нотўғри созланиши.

3. Зарарли кодлар

Зарарли код - бу бошқа дастурга унинг дастлабки ҳаракат моделини ўзгартириш ва одатда зарарли фаолият турларини амалга ошириш, масалан, маълумотлар ва шахсий маълумотларини ўғирлаш, ахборот ва ресурсларни йўқ қилиш, хизмат кўрсатишни рад этиш, спам тарқатиш ва ҳоказолар мақсадида киритилган дастур ёки дастурнинг бир қисми. Зарарли дастурнинг ҳужумларини беш туркумга бўлиш мумкин: вируслар, қуртлар, “троян дастурлари”, мобил кодлар ва аралаш дастурлар. Бир неча йиллар олдин вируслар зарарланган заиф муҳит яратиш мақсадида ёзилган бўлса, бугунги кунда зарарли кодлар мақсадли ҳужумларни амалга ошириш учун ишлатилади. Бу мавжуд зарарли кодни ўзгартириш, зарарли кодни аниқлаш технологиялари томонидан аниқланмайдиган прототипларни яратиш орқали амалга оширилади.

4. Номақбул фойдаланиш

Бундай инцидент фойдаланувчи ташкилот ахборот тизимини хавфсизлик сиёсатини бузганда юз беради. Бундай инцидентлар аслида ҳужум ҳисобланмайди, лекин кўпинча инцидент сифатида хабар берилади ва АХИТХ назорати остида бўлиши лозим. Қуйидагилар номақбул фойдаланишга мисол бўлиши мумкин:

- бузиш учун дастурларни юклаш ва ўрнатиш;
- корпоратив электрон почта қутисидан спам тарқатиш ёки шахсий бизнесини илгари суриш мақсадида фойдаланиш;
- корпоратив ресурлардан рухсат берилмаган веб-сайтни созлаш мақсадида фойдаланиш;
- марказлашмаган тармоқдан қароқчи файлларни (мусиқа, видео, дастурий таъминот) олиш ёки тарқатиш мақсадида фойдаланиш.

Фойдаланилган адабиётлар

1. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт

қоидалари

2. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар

3. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

10-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентлари соҳасида ўқитиш ва хабардор этишни таъминлаш

Режа:

1. Ахборот хавфсизлиги инцидентлари соҳасида ўқитиш ва хабардорликни ошириш
2. Ахборот хавфсизлиги инцидентлари соҳасида ҳодисаларни аниқлаш
3. Ахборот хавфсизлиги инцидентлари соҳасида ҳодисалар ҳисоботини юритиш

1. Ахборот хавфсизлиги инцидентлари соҳасида ўқитиш ва хабардорликни ошириш

Ахборот хавфсизлиги инцидентларини бошқариш - нафақат техник воситаларни, балки ходимларни ҳам ўз ичига оладиган жараёндир, демак, бу жараён ташкилотда ишлаш учун тегишли тайёргарликдан ўтган ва ахборот хавфсизлиги масалаларидан хабардор шахслар томонидан қўллабқувватланиши лозим.

Ташкилотнинг барча аъзоларининг хабардорлиги ва иштироки ахборот хавфсизлиги ҳодисаларини бошқаришга тизимли ёндашувни муваффақиятли таъминлаш учун муҳим. Фойдаланувчилар бу жараёнда иштирок этиши лозим бўлса ҳам, агар улар ахборот хавфсизлиги инцидентларини бошқаришга тизимли ёндашувдан ўзлари ва бўлинмалари қандай фойда кўришлари ҳақида хабардор бўлмасалар бундай иштирокнинг самаралилик эҳтимоли кам бўлади. Ахборот хавфсизлиги инцидентларини бошқаришга тизимли ёндашувнинг экслуатацион самараси ва сифати бир қатор омилларга, шу жумладан, инцидентлар ҳақида хабар бериш мажбурияти, ҳисобот сифатида, фойдаланишнинг осонлиги, тезлик ва ўқитишга боғлиқ. Бу омиллардан айримлари фойдаланувчилар ахборот хавфсизлиги инцидентларини бошқаришнинг аҳамиятини билишларини ва инцидентлар ҳақида хабар беришга тайёрлигини назарда тутади.

Ахборот хавфсизлиги инцидентларини бошқаришнинг роли ўқитиш ва ахборот хавфсизлиги масалаларида хабардорликни таъминлаш умумий дастурининг бир қисми сифатида фаол қўллаб-қувватланмоғи лозим. Хабардорликни таъминлаш дастури ва тегишли материал барча ходимлар, шу жумладан, яъни ходимлар, учинчи ташкилотлар ва пудратчиларнинг фойдаланувчилари учун фойдалана олинадиган бўлиши лозим. Контакт посизияси (КП), ахборот хавфсизлиги инцидентларига таъсир этиш хизмати (АХИТХ) аъзолари, зарурат бўлганда эса - ахборот хавфсизлиги учун масъул ходимлар ва маъмурлар учун махсус ўқитиш дастури бўлиши лозим. Инцидентларни бошқариш жараёнида бевосита иштирок этувчи ҳар бир гуруҳ аъзоси учун унинг ахборот хавфсизлиги инцидентини бошқариш схемасидаги иштирокининг тури, даражаси ва ҳажмидан келиб чиққан ҳолда ҳар хил тайёргарлик даражаси керак бўлиши мумкин.

Хабардорликни таъминлаш бўйича тезкор мажлис қуйидагиларни қамраб олиши лозим:

a) ташкилот ва унинг ходимлари учун ахборот хавфсизлиги инцидентларини бошқаришга тизимли ёндашувдан келиб чиқадиган афзалликлар;

b) ахборот хавфсизлиги инцидентларини бошқариш схемасининг ишлаш асосари, шу жумладан унинг ҳаракатлари доираси ва ахборот хавфсизлиги инцидентлари, ҳодисалари ва заифликларини бошқариш бўйича ишлар технологияси;

c) ахборот хавфсизлиги ҳодисалари, инцидентлари ва заифликлари ҳақидаги ҳисоботлар усуллари;

d) инцидент тўғрисида мавжуд маълумотлар ва ахборот хавфсизлиги ҳодисалари/инцидентлари/заифликлари маълумотлар омборида олинган маълумотлар;

e) манбалар махфийлигини таъминлаш механизмлари (зарурат бўлганда);

f) схема хизматининг даражалари бўйича келишув;

g) фаолият натижалари ҳақида ҳисобот юритиш - манбалар қандай шартларда хабардор қилинади;

h) ошкор қилмаслик тўғрисидаги келишувлардан келиб чиқадиган ҳар қандай чекловлар;

i) ахборот хавфсизлиги инцидентларини бошқариш ташкилотининг ваколатлари ва унинг ҳисобот берувчи линияси;

j) ахборот хавфсизлиги инцидентларини бошқариш тизими ҳисоботларини олувчилар.

Айрим холларда ахборот хавфсизлиги инцидентларини бошқариш бўйича хабардорликни таъминлаш ҳақидаги маълумотни бошқа ўқитиш дастурларига (масалан, ходимлар учун кириш дастурлари ёки ахборот хавфсизлиги масалалари бўйича хабардорликни таъминлашнинг умумий корпоратив дастурлари) махсус киритиш мақсадга мувофиқдир. Хабардорликни таъминлашга бундай ёндашув ходимларнинг айрим гуруҳлари билан боғлиқ кимматли маълумотларни тақдим қилиши ва ўқитиш дастурининг самарадорлигини яхшилаши мумкин.

Ахборот хавфсизлиги инцидентларини бошқариш тизимини ишга туширишдан олдин барча тегишли ходимлар ахборот хавфсизлиги инцидентларини аниқлаш ва ҳисобот бериш процедуралари биилан таништирмоғи, махсус танланган ходимлар эса кейинги жараёнлар бўйича яхши хабардор қилинган бўлиши лозим. Кейин хабардорликни таъминлаш бўйича мунтазам инструктаж ва тайёргарлик курслари ўтказилади. Тайёргарлик жараёнида КП гуруҳи ва АХИТХ аъзолари, шунингдек, ахборот хавфсизлиги учун масъуллар ва маъмурлар учун махсус машқлар ва назорат ўтказилиши лозим.

Бундан ташқари, ўқитиш ва хабардорликни ошириш дастурлари ахборот хавфсизлиги ҳодисалари/инцидентлари ва заифликлари ҳисоботони бериш ва қайта ишлашда сусткашликни минималлаштириш мақсадида ахборот хавфсизлиги инцидентларини бошқаришни амалга оширадиган ходимлар томонидан «кайнок линия» нинг яратилиши ва ишлаши билан тўлдирилиши

лозим.

2. Ахборот хавфсизлиги инцидентлари соҳасида ҳодисаларни аниқлаш

Ахборот хавфсизлиги воқеалари бевосита бирон-бир хавотирга сабаб бўладиган ва техник, жисмоний ва процедуравий характерга эга бўлган вазиятни сезган шахс ёки шахслар томонидан аниқланиши мумкин. Аниқлаш, масалан, ёнғин/тутун детекторлари ёки қўриқлаш сигнализацияси томонидан олдиндан белгилаб қўйилган жойларга огоҳлантириш сигналлари узатиш орқали (инсон томонидан маълум бир хатти-ҳаракатлар амалга оширилиши учун) амалга оширилиши мумкин. Ахборот хавфсизлигининг техник инцидентлари (аномал тармоқ фаоллиги, хизматнинг ишдан чиқишига мўлжалланган ҳужумлар, рухсат берилмаган маълумотни қўлга киритишга уриниш, зарарли кодни юклаш ва ҳоказо) автоматик аниқланиши мумкин, масалан, булар назорат ёзувлари таҳлили қурилмалари, тармоқлараро экранлар, ҳужумларни аниқлаш тизимлари, зарарли кодларни аниқлашнинг инструментал воситалари (шу жумладан антивирус дастурлари) томонидан юбориладиган огоҳлантириш сигналлари бўлиши мумкин, ҳар сафар сигналлар бу қурилмаларнинг олдиндан белгиланган параметрлари томонидан фаоллаштирилади.

Ахборот хавфсизлиги ҳодисаларини аниқлашнинг эҳтимолий манбаларига қуйидагилар киради:

a) фойдаланувчилар;

b) раҳбарият ва хавфсизлик хизмати раҳбарлари;

c) мижозлар;

d) ахборот технологиялари бўлими, шу жумладан Тармоқни эксплуатация қилиш маркази ва Хавфсизлик операцион маркази (2-даража қўллабқувватланиши орқали);

e) ахборот технологиялари ёрдамчи хизматлари (1-даража қўллаб қувватланиши орқали);

f) бошқариладиган хизматлар провайдерлари (шу жумладан интернет провайделар ва телекоммуникациялар хизматлари провайдерлари);

g) АХИТХ;

h) ҳар кунги иши давомида аномалияларни аниқлаши мумкин бўлган бошқа бўлинмалар ва ходимлар;

i) ОАВ (газеталар, телевидение ва ҳоказо);

j) веб-сайтлар (ахборот хавфсизлиги бўйича веб-сайтлар, хавфсизликни тадқиқ килувчилар веб-сайтлари ва ҳоказо).

3. Ахборот хавфсизлиги инцидентлари соҳасида ҳодисалар ҳисоботини юритиш

Ахборот хавфсизлиги ҳодисасини аниқлаш манбаидан қатъий назар, ноодатий нарсага эътибор қаратган ёки автоматик воситалар томонидан хабардор қилинган шахс аниқлаш ва ҳисобот жараёнини бошлаш учун масъул бўлади. Бу шахс ташкилотда доимий ёки хизмат шартномаси асосида ишлаётган ҳар қандай ходим бўлиши мумкин.

Бу вакил биринчи навбатда КП ва раҳбариятнинг эътиборини жалб қилиш мақсадида ахборот хавфсизлиги инцидентларини бошқариш схемаларида белгиланган процедураларга риоя қилиши ва ахборот хавфсизлиги ҳодисалари ҳақидаги ҳисобот шаклларини ишлатиши лозим. Демак, барча ходимлар ахборот хавфсизлиги эҳтимолий ҳодисалари ҳақида хабардор қилиш масалаларига тегишли тавсиялар, шу жумладан, ҳисобот шакллари билан танишган бўлиши ва ахборот хавфсизлиги ҳодисасининг ҳар бир юзага келиш ҳолати ҳақида хабардор қилиниши лозим бўлган ходимларни таниши мумкин. Бунга ахборот хавфсизлиги ҳодисалари ҳақидаги ҳисоботлар шакллари ва ҳар бир инцидент ҳақида огоҳлантирилиши лозим бўлган шахслар ҳақидаги маълумотлар киради (барча ходимлар хеч бўлмаганда ҳисобот шакллари ҳақида хабардор қилиниши лозим, бу уларнинг ахборот хавфсизлиги инцидентларини бошқариш схемасини тушунишларига ёрдам беради).

Шуни таъкидлаш лозимки, эшитилишдан ҳимоя қилинган стационар, симсиз ёки мобил телефон хавфсиз эмас. Махфий ахборот билан ишлаётганда қўшимча ҳимоя чоралари кўрилиши лозим.

Қуйидаги маълумотлар инцидентларни кузатиш тизимларида қайд шакллари учун асос бўлиб хизмат қилиши мумкин:

- аниқланган вақт/сана;
- кузатувлар;
- боғланиш учун маълумотлар (мажбурий эмас).

Тўлдирилган шакл (қоғозда ёки электрон почта орқали ёки веб-шакллар орқали тақдим қилинган) АХИТХ ходимлари томонидан фақат ахборот хавфсизлиги инцидентларини инцидентларни кузатиш тизимларида қайддан ўтказиш пайтида ишлатилиши лозим. Эҳтимолий/содир бўлиб ўтган/аниқланган ахборот хавфсизлиги ҳодисалари ҳақида маълумотлар/ҳисоботлар олиш муҳим.

Ахборот хавфсизлиги ҳодисаларини (эҳтимолий инцидентларини) кузатиш иложи борича автоматлаштирилган дастурлар томонидан амалга оширилиши лозим. Ахборот тизимларини кўллаш ходимларни ўрнатилган процедуралар ва назорат руйхатларига риоя қилишга мажбурлаш учун муҳим. Шунингдек, «ким нима ва качон килганлигини» ҳамда ахборот хавфсизлиги ҳодисаси (эҳтимолий инциденти) пайтида ҳато туфайли тушириб қолдирилиши мумкин бўлган тафсилотларни кузатиб бориш фойдалидир.

Конкрет ахборот хавфсизлиги ҳодисасини қайта ишлаш бу ҳодиса нимадан иборатлигига ҳамда олиб келиши мумкин бўлган оқибатлар ва таъсирларга боғлиқ. Кўпчилик учун ҳодисани қайта ишлаш усули ҳақида қарор қабул қилиш уларнинг ваколатларига кирмайди. Шунинг учун ахборот хавфсизлиги ҳодисаси ҳақида хабар бераётган ходим шаклни шундай тўлдириши керакки, унда ўша пайтда маълум бўлган иложи борича кўпроқ ахборот акс этиши керак. Зарурат бўлганда ходим ўз раҳбари билан боғланади. Бу шаклларни хавфсиз усул билан тегишли КПга (суткасига 24 соат, хафтасига 7 кун ишлайдиган) узатиши керак, хабарнинг нусҳаси эса масъул АХИТХ га узатилиши керак. Ахборот хавфсизлиги ҳодисаси ҳақидаги ҳисобот намунаси D иловада келтирилган.

АХИТХ электрон почта, телефон, факс орқали юборилган барча

ҳисоботлар учун масъул ходим ёки вакилни тайинлаши керак. Бу масъулият хизмат ходимлари орасида ҳар хафта ўтиб туриши мумкин. Хизматнинг тайинланган ходими вазиятни баҳолайди ҳамда масъул ва манфаатдор томонларни хабардор қилиш учун, шунингдек, ахборот хавфсизлиги инцидентларини бартараф қилиш учун зарур чораларни кўради.

Шуни алоҳида таъкидлаш лозимки, ҳисобот шаклларини тўлдиришда нафақат мазмуннинг аниқлиги, балки вақтида тўлдирилиши ҳам жуда муҳим. Шунингдек ахборот хавфсизлиги ҳодисаси ҳақидаги ҳисоботни юборишни унинг мазмунига аниқлик киритиш мақсадида кечга қолдириб ҳам бўлмайди. Агар хабар берувчи ҳисобот шаклининг бирон-бир қисмидаги маълумотга ишончи комил бўлмаса, бу қисмни белгилаб қўйиш керак ва маълумотни кейинчалик аниқлаштириб жўнатиш лозим. Шуни ҳам тан олиш лозимки, электрон айрим электрон ҳисобот механизмлари (масалан, электрон почта) ўзи ҳам хужумга нишон билиши мумкин.

Одатий ишлатиладиган электрон ҳисобот механизмлари (масалан, электрон почта) билан муаммолар мавжуд бўлганда ёки муаммолар мавжудлигига шубҳа бўлган тақдирда, шунингдек, тизимга ҳужум бўлганда ва ҳисоботлар ваколати бўлмаган шахслар томонидан ўқилганда алтернатив алоқа воситалари ишлатилиши лозим. Алтернатив алоқа воситаларига ходимлар, телефонлар ёки матнли хабарлар кириши мумкин. Бундай алтернатив алоқа воситалари терговнинг илк босқичларида, ахборот хавфсизлиги ҳодисаси ахборот хавфсизлиги инциденти сифатида таснифланиши аниқ бўлганда, айниқса, бундай ахборот хавфсизлиги инциденти муҳим деб саналадиган пайтда ишлатилиши лозим.

Ахборот хавфсизлиги инциденти тезда ёлғон риск сифатида аниқланиши ёки қониқарли ечимга олиб келиниши мумкин. Бундай холларда ҳисобот шаклларини тўлдириш ҳамда КП ва АХИТХ нинг маҳаллий раҳбариятига қайд қилиш мақсадида, яъни ахборот хавфсизлиги ҳодисалари/инцидентлари/заифликлари маълумотлар омборига киритилиши учун жўнатиш лозим. Бундай ҳолда ахборот хавфсизлиги ҳодисаси ёпилгани

ҳақида хабар берувчи шахс ахборот хавфсизлиги инцидентлари ҳақидаги ҳисобот шаклларини тўлдириш учун талаб қилинадиган маълумотларни узатиши мумкин - бунда ахборот хавфсизлиги инциденти ҳақидаги ҳисобот шакли тўлдириб, тегишли органларга жўнатилиши лозим. Автоматик инструментал воситаларни кўллаш айрим маълумотларни тўлдиришда, масалан, вақтни кўрсатишда, шунингдек, керакли ахборот алмашиш/узатишда фойдали бўлиши мумкин.

Фойдаланилган адабиётлар

1. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари
2. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар
3. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.
4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

11-маъруза.

Mavzu: Ахборот хавфсизлиги инцидентларини тергов этиш. Ахборот хавфсизлиги инцидентлари даллиларини сақлаш.

Режа:

1. Ахборот хавфсизлиги инциденти тергови тушунчаси ва содир этганлик учун жавобгарликлар
2. Ахборот хавфсизлиги инцидентларини тергов қилиш жараёнидаги қаршиликлар
3. Инцидент содир бўлган жойни кўздан кечириш ва даллиларини тўплаш ҳамда сақлаш

1. Ахборот хавфсизлиги инциденти тергови тушунчаси ва содир этганлик учун жавобгарликлар

Ҳозирги кунда компьютер технологияларининг тарқалиши одатий ҳолга айланиб, бугун бирор-бир корхона ёки ташкилот фаолиятини компьютер воситаларисиз тасаввур қилиш қийин. Улар янги ва янги фаолият доираларига жорий қилинмоқда, улар зиммасига янада аҳамияти, жиддийроқ бўлган масалалар юклатилмоқда.

Аммо дунё миқёсида тобора кенгайиб бораётган илмий-техникавий ривожланиш жараёнлари билан бир қаторда, илгари мавжуд бўлмаган жиноятларнинг турлари, шакллари ва кўринишлари юзага келмоқда, яъни ахборот технологиялари соҳаси билан боғлиқ жиноятлар вужудга келиб, уларнинг сони ҳам, тури ҳам ортиб бормоқда. Ушбу ҳолат, ўз навбатида, қонун чиқарувчидан кечиктириб бўлмайдиган чоралар кўришни талаб қилди. Бинобарин, бу борада мамлакатимизда кўпгина ишлар бажарилди ва ахборот тизимлари соҳасидаги жиноятчиликнинг олдини олиш ва унга қарши кураш фаолиятини тартибга солувчи бир қатор норматив-ҳуқуқий ҳужжатлар қабул қилинди.

Ўзбекистон Республикасининг «Ахборот олиш кафолатлари ва эркинлиги тўғрисида»ги, «Ахборот эркинлиги принциплари ва кафолатлари

тўғрисида»ги, «Ахборотлаштириш тўғрисида»ги қонунлари, Вазирлар Маҳкамасининг «Электрон рақамли имзодан фойдаланиш соҳасида норматив-ҳуқуқий базани такомиллаштириш тўғрисида»ги қарори 5 ва бошқалар шулар жумласидандир.

Ўзбекистон Республикасининг 2007 йил 25 декабрдаги қонуни билан илк бор миллий жиноят қонунчилигимиз, яъни Жиноят кодекси Махсус қисми XX-бобида ахборот технологиялари соҳасидаги ижтимоий хавфли қилмишлар учун жиноий жавобгарликни назарда тутувчи жиноий-ҳуқуқий нормалар киритилди.

Жиноий жазо назарда тутилган нормаларга:

- ахборотлаштириш қоидаларини бузиш (278^1-м);
- компьютер ахборотидан қонунга хилоф равишда (рухсатсиз) фойдаланиш (278^2-м); компьютер тизимидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш (278^3-м);
- компьютер ахборотини модификациялаштириш (278^4-м);
- компьютер саботажи (278^5-м); зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш (278^6-м) киради.

Шундай қилиб, ахборот технологиялари соҳасидаги муносабатлар жиноий-ҳуқуқий ҳимояга эга бўлиб, бунинг оқибатида ёпиқ (конфиденциал) ахборотлар жиноятнинг янги объекти сифатида шаклланди. Ушбу жиноятларни ўзига хослигини инобатга олган ҳолда тергов қилиш методикасини ишлаб чиқиш – бугунги кунда долзарб муаммолардан бири бўлиб турибди.

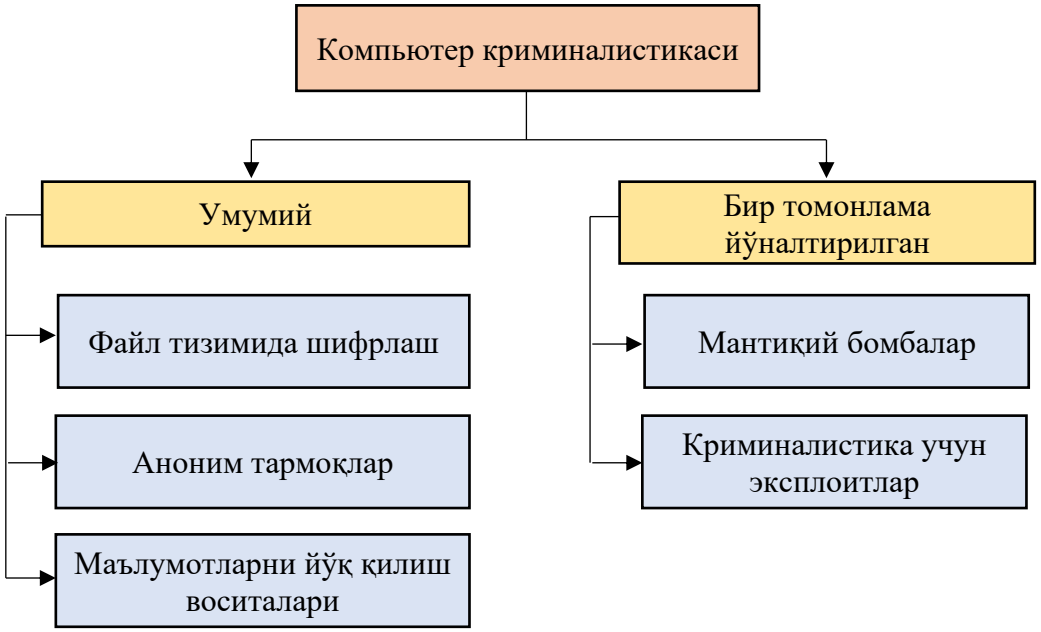
Жиноят процессида кўздан кечириш тергов ҳаракати энг муҳим ва жиноят бўйича энг кўп ахборот тўплай олиш имконини берадиган тергов ҳаракатларидан бири ҳисобланади.

Бундан ташқари, тергов ҳаракатига ахборот технологиялари соҳасидаги мутахассисни жалб қилиш имкони бўлмаганида инцидент жойида терговчининг алоҳида эътибор бериши лозим бўлган ҳолатлар ва тергов-

тезкор гуруҳи раҳбари сифатида амалга ошириши лозим бўлган вазифалари ёритилган.

2. Ахборот хавфсизлиги инцидентларини тергов қилиш жараёнидаги қаршиликлар

Ахборот хавфсизлиги инцидентларини тергов қилиш даражасида бузғунчи томонидан қаршиликларга учраш мумкин. Бундай ҳаракат бир томонлама йўналтирилган ёки умумий бўлиши мумкин (11.1-расм).



11.1-расм. Компьютер криминалистикаси

Умумий қарши ҳаракатлар. Умумий қарши харакатлар кимгадир ёки нимагадир йўналтирилмаган бўлиб кўпчилик ҳолларда икки хил вазифани бажарувчи ресурслардан фойдаланилади (мисол, файл тизими шифрлашини яратувчи дастурлар ёки тармоқ трафигини шифрловчи дастурлар). Ушбу қарши ҳаракатнинг асосий мақсади маълумотларни шифрлаш, йўқ қилиш ёки яшириш йўллари билан криминалистик тадқиқотлардан ҳимоя қилишдир.

Йўналтирилган қарши ҳаракат ёки криминалистик ҳаракатни алдаш, ушбу ҳаракатнинг асосий йўналишларидан бири ҳисобланади. Ушбу турнинг асосий мақсади: криминалистик изланишлардан маълумотларни сақлаш, криминалистик усуллар ишончсизлигини кўрсатишдир.

Ушбу ҳаракатнинг бошқа турида криминалистик текширув олиб

бораётган ташкилот тармоғига рухсатсиз кириб маълумотларга ўзгартириш киритишдан иборат ҳисобланади (бунинг учун дастурлар ва қурилмаларнинг заиф қисмларидан фойдаланилади). Энг кўп тарқалган усуллардан бири бу умумий қаршилик ҳаракатлари ҳисобланади. Мақсадга йўналтирилган қарши ҳаракатлар кам ўрганилган бўлим ҳисобланади.

Қаршилик ҳаракатларининг умумий усуллари. Энг кўп тарқалган қаршилик ҳаракатларидан бири бу- маълумотларни ҳимоялаш бу-шифралаш, стенографик яшириш, қайта ёзиш ёки ўчириб ташлаш ҳисобланади.

Шу билан бирга ҳозирги кунда криминалистик изланишларда мумкин бўлган маълумотларни йўқ қилишга қаратилган усуллар ҳам кўпдир. Бундай дастурлар оператив хотирада ишлайди. Бундай усуллар ва дастурлар кўп ҳолларда шахсий маълумотларни конфиденциал(махфий) сақлаш учун ёки сўз эркинлигини сақлаб қолиш учун ишлатилади.

Юқорида санаб ўтилган усуллар қўлланилиши кибержиноятни очиш учун катта тўсиқ ҳисобланади, аммо бир қанча криминалистик усуллар мавжудки улар шундай ҳимояланган маълумотларни топиш ва очиш учун мўжалланган ҳисобланади.

Инцидентларни терговга қарши мақсадга йўналтирилган усуллар. Мақсадга йўналтирилган усуллар криминалистик қийматга эга бўлган маълумотларни аниқлаш ва уларни йўқ қилишдан иборат ҳисобланади. Криминалистик терговни аниқлаш эса бир қанча усуллардан фойдаланган ҳолда амалга оширилиши мумкин: тармоқ воситаларини ишлаш аломатларини қидириш мақсадида тармоқ трафигини таҳлили, ишлаётган дастурлар таҳлили ва ҳ.к.

Бир томонлама йўналтирилган ҳаракатлар. Маълумотларни йўқ қилиш, яшириш ёки ўзгартириб қўйиш мантиқий бомбалардан ёки криминалистик дастурларга қарши эксплоитлардан фойдаланишлар орқали амалга оширилади(бундай воситалар дастур хатоликларидан фойдаланиши мумкин).

Йўналтирилган қаршилик кўрсатиш асосан криминалистиканинг

қуйидаги заиф жойларига ҳужум қилиши мумкин:

1. Усул.
2. Восита.
3. Ҳаракат.

Усул - компьютер маълумотларини ўрганиб чиқиш учун умумий усуллар. Масалан: криминалистик операцион тизим юкланиши, у ўз навбатида нусхалашдан ҳимояланмаган тарзда ишга туширилади, кейинчалик керакли файллардан нусха олиш учун ҳам ишлатилади.

Восита - дастур ёки қурилма ҳисобланиб, криминалистик изланишларнинг маълум даражасида фойдаланилади. Мисол: Криминалистик Live CD grml.

Ҳаракат - маълум бир даражадаги мақсадга йўналтирилган ҳаракатлар кетма кетлигидир. Масалан: файлларни нусхалаш учун дастур ишга туширилиши (натижа: дискда мавжуд бўлган файллар нусхаланиши) файлларни индекслаш учун дастурни ишга тушириш (натижа керакли файлни калит сўзлар ёрдамида тездо топиб олиш).

Юқорида келтирилган заиф нуқталарга қарши қуйидаги ҳаракатларни келтиришимиз мумкин:

1. Карши ҳаракат қурилмада махсус файллар яратиш орқали: криминалистик изланиш аниқланса дархол файлни алмаштириб қўйиш.
2. Дастурий воситалар ёрдамида қаршилик кўрсатиш.
3. Криминалистик изланиш олиб борилгани ҳақида факт маълум бўлгач криминалистик ишлаётган дастурлар турларини аниқлаш.

Аппарат (ёрлиқлар). Кўпчилик криминалистик ҳаракатларга қарши қўллаш мумкин бўлган усуллардан бири аппарат ёрлиқлар ҳисобланади. Маласан, криминалистик изланишлар олиб борилиши аниқлангандан сўнг файлга ўзгартиришлар киритиш ёки йўқ қилиш бу аппарат ичига киритилган ёрлиқ ҳисобланади. Бундай услуб билан Live CD ёки дастурий модуллардан қутилиш учун фойдаланиш мумкин. Бошқа мисол эса маълумотларни аппаратли йўқ қилиш ҳисобланади. Бунда кутилмаган тарзда маълумот сақлаш

қурилмасини очишга уринишдир. Бундай ҳолатларда батарея ишга тушади ва узоқ вақт давомида кучли ток билан таъсир ўтказади.

Дастурий (ёрлиқлар). Яқин кунларгача дастурий ёрлиқлар фақатгина баъзи ҳолларда ўзини яхши кўрсата олар эди. Масалан Live CD дискка ёзишдан ҳимояланмаган ҳолда компьютерни ишга тушириши мумкин. Хозирги кунда эса улар маълум бир криминалистик изланишларга ҳам қарши тура оладиган дастурий восита сифатида фойдаланилмоқда.

3. Инцидент содир бўлган жойни кўздан кечириш ва даллиларини тўплаш ҳамда сақлаш

Ахборот технологиялари соҳасидаги жиноятлар бўйича ўтказиладиган инцидент содир бўлган жойни кўздан кечириш тергов ҳаракати энг муҳим ва жиноят бўйича энг кўп ахборот тўплаш имконини берадиган тергов ҳаракатларидан бири ҳисобланади. Ушбу тергов ҳаракати бир қатор муҳим шароитларни, жумладан:

- ўрганилаётган инцидентни асосий хусусияти, унда жиноят таркиби мавжудлиги;
- жиноятнинг содир этилган жойи ва вақти; жиноятда иштирок этганларнинг ҳаракатлари нимадан иборат бўлганлиги;
- мақсадлар ва мотивлар; инцидент содир бўлган жойда қандай предметлар ёки нарсалар қолдириб кетилганлиги;
- жиноят содир этган шахслар қандай қилиб инцидент содир бўлган жойга кириб чиққанлиги, у ерда қанча вақт бўлганлиги;
- тажовуз предметига етиб бориш ва у билан ноқонуний ҳаракатлар содир этиш учун қандай техника воситалари ва ҳужжатлардан фойдаланилганлиги;
- реал воқеаларни яшириш учун қандай ҳаракатлар амалга оширилганлиги;
- салбий оқибатлар ва уларнинг излари юзага келишини қаердан излаш лозимлиги;

- салбий натижаларни юзага келишига нима сабаб бўлганлиги ва бошқаларни аниқлаш имконини беради.

Шуни таъкидлаш жоизки, «инцидент содир бўлган жой» ва «жиноят жойи» бир хил бўлмаслиги мумкин. Жиноий ҳаракат бир жойда, масофадан компьютер тармоқлари орқали содир қилинган бўлиши мумкин, унинг оқибатлари эса бошқа жойда юзага келади.

Аниқ тергов вазиятга қараб тергов-тезкор гуруҳи таркибига қуйидаги ходимлар киради:

– ахборот соҳасидаги жиноятларни тергов қилишга ихтисослашган терговчи (тергов-тезкор гуруҳи раҳбари);

– ахборот технологиялари соҳасидаги жиноятларга қарши кураш бўлими ходими;

– жиноят содир бўлган ҳудудга бириктирилган тезкор ходим;

– ушбу турдаги жиноятларнинг изларини топиш, тадқиқ қилиш, қайд этиш ва олиш соҳасидаги маълум билимга эга бўлган криминалист-мутахассис;

– тергов ҳаракати жараёнида кўздан кечирилиши лозим бўлган ҳисоблаш техника воситаси бўйича мутахассис;

– жиноят излари топилганда ўтказилган технологик жараён ҳақида етарли билимларга эга бўлган мутахассис;

– жиноят таъсирига дуч келган рақамли ахборот (унинг рақамли ахборот ташувчиси ёки ҳисоблаш техника воситаси) учун моддий жавобгар шахс;

– аризачи ёки жабрланувчи.

Юқорида кўрсатилган тергов-тезкор гуруҳи аъзолари терговчига атроф муҳитни ўрганиш ва қайд этиш; далилларни топиш, қайд этиш, олиш ва сақлаш; инцидент содир бўлган жойда керакли далилларни дастлабки тадқиқ этиш; келгуси тадқиқотлар учун керак бўладиган объектларни ажратиб олиш; жиноят содир бўлишига имкон берган шароитларни аниқлаш; баённомада ўзига хос бўлган изларни ёритиб бериш; тергов ҳаракати жараёнида техник воситаларни ишлатиш; режа, чизмалар ва схемалар тузиш; жиноятчиларни,

гувоҳларни ва жабрланувчини қидиришда самарали йўналиш танлаш ва ҳоказоларда ёрдам кўрсатади.

Мазкур тергов ҳаракати олдиндан тайёрланиб, батафсил режалаштирган бўлиши керак. Дастлаб қуйидаги ишларни амалга ошириш мақсадга мувофиқ:

– вужудга келган тергов вазиятидан келиб чиққан ҳолда тергов ҳаракатида иштирок этувчи шахсларни аниқлаш;

– ҳар бир тергов-тезкор гуруҳи аъзосига мақсадлар ва ҳаракатлар кетма-кетлигини аниқ ва равон белгилаб бериш;

– тегишли мутахассисларни жалб қилиш ва уларга керак бўладиган техник воситаларни олиб келишларини уқтириш (терговчи ва эксперт-криминалистнинг ихтиёрида бўлган техник воситалардан ташқари);

– тергов ҳаракатини бошлашдан олдин иштирокчиларга уларнинг ҳуқуқ ва мажбуриятларини, қўйилган мақсадни, шунингдек инцидент содир бўлган жойда ҳаракатланишда ва махсус моддалар билан ишлашда эҳтиёт чораларини тушунтириб ўтиш;

– холисларни танлаб олиш, йўриқнома ўтказиш ҳамда ҳуқуқ ва мажбуриятларини тушунтириш. Холисларни танлашда компьютер ахбороти соҳасида етарли (ўртача шахсий компьютер фойдаланувчининг билимидан паст бўлмаган) билимларга эга бўлган шахсларни жалб қилиш мақсадга мувофиқдир.

Тергов-тезкор гуруҳи инцидент содир бўлган жойга етиб келганидан сўнг терговчи томонидан қуйидаги ишлар амалга оширилиши лозим:

1. Инцидент содир бўлган жойга ишга алоқаси бўлмаган шахсларни киришини ва объектнинг қўриқланишини таъминлаш. Бундан шартли равишда қуйидагилар қўриқланиши лозим:

а) инцидент содир бўлган жой ҳудуди;

б) жиноят излари аниқланган ҳисоблаш техника воситаси ўрнатилган жой;

с) технологик жараённи бошқарадиган ва охирги операциялар тўғрисида маълумотларни сақлайдиган локал тармоқ сервери;

д) электр ток манбаини ўчириш нуқталари (агар техника воситалари

ёқилган ҳолатда бўлган тақдирда).

Ушбу вазиятда қуйидагилар эътиборга олиниши керак: ҳисоблаш техника воситасининг клавиатурасида ишлаш, уни электр ток манбаидан ўчириш (ёки ёқиш), локал тармоқ сервери билан ва периферик воситалар билан алоқани узиш (ёки улаш) – компьютер ахборотининг, рақамли ахборот ташувчиларнинг ва қоғозли ҳужжатларнинг ўзгариши ёки ўчирилишига олиб келиши мумкин. Шунинг учун тергов ҳаракати бошланишида ҳисоблаш техника воситаси ёки бошқа электрон восита ёқилган (ўчирилган) ҳолатда бўлса, у тегишли мутахассис томонидан кўздан кечириш тамом бўлгунга қадар ўз ҳолатида қолиши лозим.

2. Юз берган воқеанинг асл мазмуни, инцидент содир бўлган жойда мавжуд бўлган жиҳозларнинг ўзгариши, ҳар бир шахснинг тергов-тезкор гуруҳи келгунга қадар бўлган ҳаракатларига аниқлик киритиш мақсадида жабрланувчи (аризачи), моддий жавобгар шахс ва гувоҳларни сўроқ қилиш (инцидент содир бўлган жойни батафсил кўздан кечириш жараёнида аниқланадиган саволлар ойдинлаштирилади);

3. Тергов-тезкор гуруҳи инцидент содир бўлган жойга етиб келганда юзага келган вазиятни баённомада қайд этиш, ориентирли ёки обзорли фото ёки видеоёзувни амалга ошириш;

4. Инцидент содир бўлган жойга чиққан тергов-тезкор гуруҳи аъзоларига топшириқлар бериш. Хусусан:

а) ҳудудий тезкор вакилга – инцидент содир бўлган жойни чизмасини тузиш, ушбу чизмада инцидент содир бўлган жойни кўздан кечириш жараёнида аниқланган барча излар ўз аксини топиши лозимлигини тушунтириш. Чизма тузишда ҳисоблаш техника воситалари бир-бирига ва периферик воситаларга уланганлик ҳолати, компьютер ахборотига кириш ҳуқуқини чегараловчи қўриқлаш тизимлари, турли хил видео кузатув қўриқлаш тизими элементлари ва бошқа ҳолатларни аниқлашда амалий ёрдам кўрсатиш учун тергов ҳаракатига жалб қилинган мутахассис бириктирилиши мақсадга мувофиқ. Бундан ташқари, ҳудудий тезкор вакилга бир қатор тактик

операцияларни ўтказиш тўғрисида топшириқ бериш (жиноятни иссиқ изидан очиш, ушланган шахснинг шахсий тинтуви, аризачи ва гувоҳларнинг сўрови ва ҳоказо);

b) эксперт-криминалистга жиноят изларини аниқлаш бўйича вазифалар юклаш;

c) тергов ҳаракати жараёнида кўздан кечирилиши лозим бўлган ҳисоблаш техника воситаси бўйича мутахассисга ҳисоблаш техника воситасининг турини, ишлатилиш мақсади, алоқага чиқиш имкониятларини аниқлаш, шунингдек ушбу воситанинг хотирасида мавжуд бўлган электрон ҳужжатларни ва ишга аҳамиятли бўлган бошқа компьютер ахборотларини олишда ва баённомада қайд этилишида терговчига амалий ёрдам кўрсатиш каби вазифалар юклатилади.

Ахборот соҳасидаги жиноятлар бўйича инцидент содир бўлган жойни кўздан кечиришни ўтказишда “марказдан четга” (эксцентрик) тактик усулини қўллаш мақсадга мувофиқдир.

Ушбу жараёнда, инцидент содир бўлган жойнинг турига қараб, “марказ” бўлиб жиноят содир этилиши мумкин бўлган ҳисоблаш техника воситаси ўрнатилган жой ёки жиноят содир этилиши учун тайёрланган восита ишлаб чиқарилган иш жойи бўлиши мумкин.

Тергов ҳаракати натижасида тузиладиган инцидент содир бўлган жойни кўздан кечириш баённомасида қуйидагиларга эътибор бериш лозим:

1) кўздан кечирилаётган объектнинг номланиши ва вазифаларига;

2) кўздан кечирилаётган объектнинг ҳудудий жойлашиши, унга кириш йўллари, унинг атрофидаги иншоатлар ва уларгача бўлган масофага;

3) объектнинг қўриқлаш тизими мавжудлигига, мавжуд бўлса, унинг жойлашиши ва ташқи кўринишига, шунингдек компьютер ахбороти чиқиб кетишига қарши қаратилган махсус ҳимояловчи сигнал воситаларига;

4) жиноят содир этилиши мумкин бўлган ҳисоблаш техника воситасининг иншоатдаги эшик, ойна, бошқа ҳисоблаш техника воситалари, видео кузатув ускуналари (мавжуд бўлган тақдирда) ва бошқаларга нисбатан жойлашиши;

5) тергов қизиқиш уйғотган ҳисоблаш техника воситасидан ташқари, хонада мавжуд бошқа ҳисоблаш техника воситалари ва электр ускуналарга;

6) жиноят содир этилган ҳисоблаш техника воситасининг алоқа каналлари ёки бошқа ҳисоблаш техника воситалари билан уланадиган техник воситалари мавжудлигига;

7) жиноят содир этилиши мумкин бўлган ҳисоблаш техника воситасининг бошқа хоналардаги ҳисоблаш техника воситалари билан уланадиган техник воситалари мавжудлигига (мавжуд бўлган тақдирда инцидент содир бўлган жойни кўздан кечириш чегаралари анча кенгайиши мумкин);

8) объектда, унга келиш-кетиш йўлларида жиноятчи қолдирган изларга;

9) кўздан кечирилаётган ҳисоблаш техника воситасининг ҳужжатлари мавжудлигига.

Юқоридагилардан шуни хулоса қилиш мумкинки, ахборот технологиялари соҳасидаги жиноятлар бўйича инцидент содир бўлган жойни кўздан кечириш тергов ҳаракатидан ташқари комплекс тезкор-қидирув ва текширув тадбирлари ўтказилади, бу эса кечиктириб бўлмайдиган бошқа тергов ҳаракатлари ўтказилишига олиб келиши мумкин, жумладан: тинтув, олиб қўйиш, ҳужжат ва предметларни кўздан кечириш, ушлаб туриш, сўроқ қилиш, таниб олиш учун кўрсатиш ва бошқалар.

Фойдаланилган адабиётлар

1. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари
2. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар
3. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.
4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для

вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

12-маъруза.

Мавзу: Ахборот хавфсизлиги инцидентларини назорат этувчи воситаларнинг таҳлили

Режа:

1. Ўзбекистон Республикасида ахборот хавфсизлиги инцидентлари ҳолатини таҳлил этиш
2. Америка, Европа ва Осиё давлатларида ахборот хавфсизлиги инцидентлари бўйича амалга оширилган ишлар мазмуни
3. Ахборот хавфсизлиги инцидентларини назорат этувчи воситалар турлари
4. Ахборот хавфсизлиги инцидентларини назорат этувчи воситаларнинг тахлили

1. Ўзбекистон Республикасида ахборот хавфсизлиги инцидентлари ҳолатини таҳлил этиш

CERT-Computer emergency response team. Фавқулотдвги вазиятларда компьютерли жавоб қайтариш гуруҳи.

Биринчи Президентимиз Ислом Каримовнинг 2005-йил 5-сентабрда қабул қилинган “Миллий ахборот-коммуникация тизимларининг компютер хавфсизлигини таъминлаш борасидаги қўшимча чора-тадбирлар тўғрисида”ги қарори ижросини таъминлаш доирасида Компютер ва ахборот технологияларини ривожлантириш ҳамда жорий етиш маркази (Uzinfocom) ҳузурида Компютер ҳодисаларига чора кўриш хизмати (UZ-CERT) ташкил етилди.

Бугунги кунда миллий ахборот тизимларимиз ва интернетдан фойдаланувчилар учун ягона марказ бўлган ушбу хизмат томонидан ахборот тўплаш, таҳлил қилиш, маслаҳат бериш ҳамда техник кўмаклашиш борасида салмоқли ишлар амалга оширилмоқда.

Миллий ахборот тизимлари ва интернетдан фойдаланувчилар учун

ягона марказ бўлган UZ-CERT томонидан ахборот тўплаш, таҳлил қилиш, маслаҳат бериш ҳамда техник кўмаклашиш борасида салмоқли ишлар амалга оширилмоқда.

UZ-CERT хизмати мутахассисларининг айтишича, барча ташкилот фаолиятини батафсил ўрганиш, мувофиқлаштириш кибер-таҳдидларга қарши курашга ёрдам бермоқда. Интернет-фирибгарлик ёки фойдаланувчилар махфий маълумотларидан ноқонуний фойдаланиш энг кенг тарқалган ана шундай хавфлардан ҳисобланади. Бундай қинғир мақсадларга, одатда, сервис ичида машҳур брендлар номидан электрон хатлар ва шахсий маълумотларни оммавий тарқатиш орқали эришилади.

Кибер-жиноят бутун дунёда оддий жиноятларга тенглаштирилмоқда, уларни содир этган шахслар эса қонун бўйича жазоланмоқда. Жиноятга дахлдорлиги экспертиза томонидан аниқланадиган компьютер, ахборот манбалари – дисклар, флешкалар, IP-манзиллар, тармоқ ускуналари тегишли айбларни қўйишда далил бўлиши мумкин. UZ-CERT хизмати ходимлари кибер-жиноятни текширишда жиноят изини яшириш мақсадида йўқ қилинган маълумотларни қайта тиклайди.

UZ-CERT хизмати ҳолатларини таҳлили.

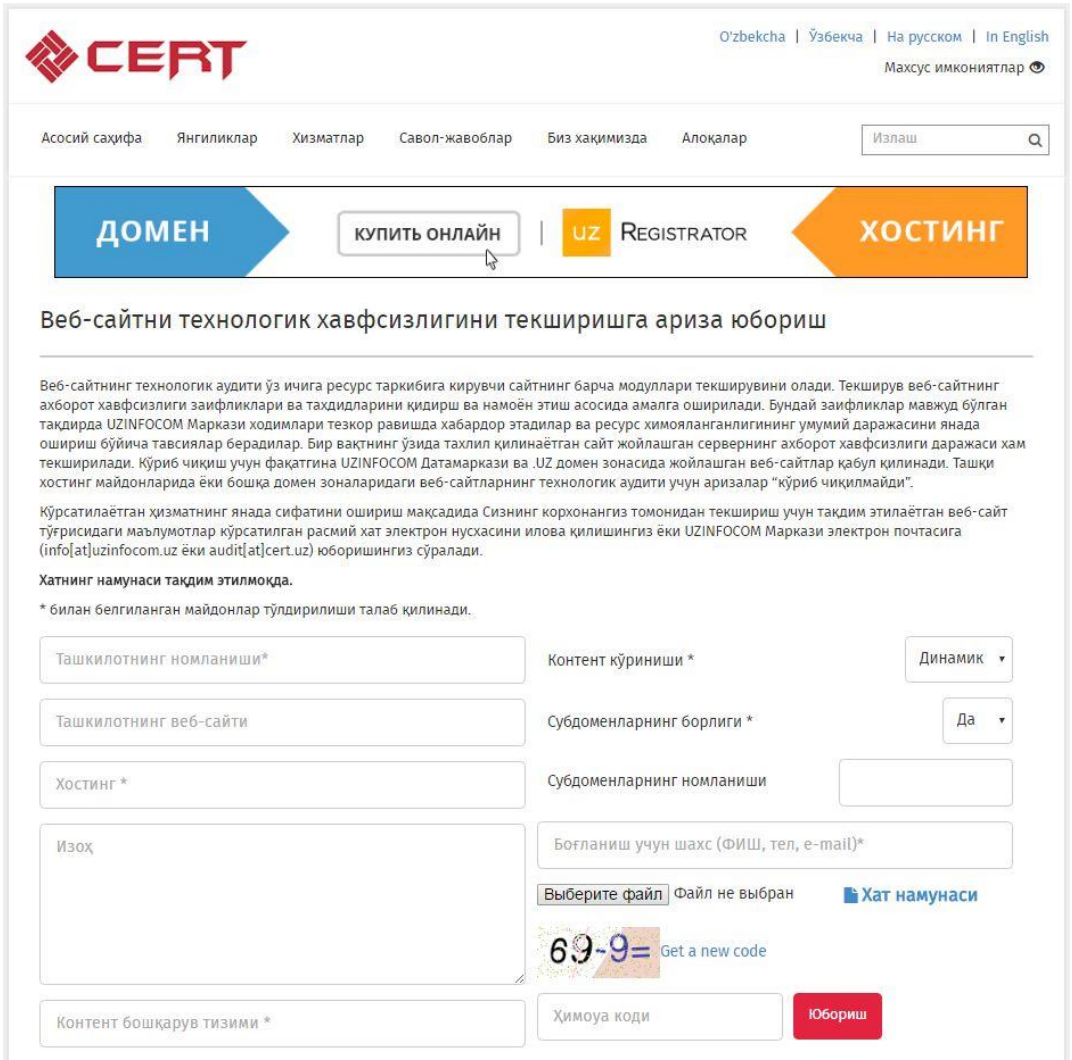
Мавжуд ресурлардан самарали фойдаланиш учун ва ахборот тизимлари, Датамарказда жойлашган мижоз веб-сайтларини ва UZINFOCOM Маркази хизматлари истеъмолчиларини химояланганлик даражасини ошириш максадида, ҳамда зарарли компютер инцидентларига тезкор жавоб кўриш ва уларнинг оқибатлари ва сабабларини бартараф қилиш мақсадида UZINFOCOM Марказида UZ-CERT (UZINFOCOM Марказининг компютер инцидентларига тезкор жавоб қайтариш хизмати) номи остида техник хавфсизлик бўлими хизмат кўрсатмоқда.

UZ-CERT хизмати Датамарказ мижозларига юқори даражали хизматлар кўрсатишга йўналтирилган. Бундан ташқари сўров асосида корхоналар ва ташкилотларнинг ахборот тизимларини хавфсизлигини таъминлаш ва рўй берувчи компютер ходисаларини бартараф этиш ва олдини олишда

кўмаклашиб келмоқда. Шуни таъкидлаш лозимки UZ-CERT хизмати давлат назорат органи эмас ва текширишлар натижалари тавсия характерига эга.

Бугунги кунда мавжуд кўрсатиладиган хизматлар рўйхатига қуйидагилар киради:

- Ахборот хавфсизлиги экспертизасини ўтказиш;
- Ахборот хавфсизлиги сиёсатини ишлаб чиқиш;
- Веб-сайтни технологик хавфсизлигини текшириш;
- Файлларни вирусдан текшириш;
- Серверлардаги ахборот хавфсизлиги ҳолати анализи хамда бошқалар.



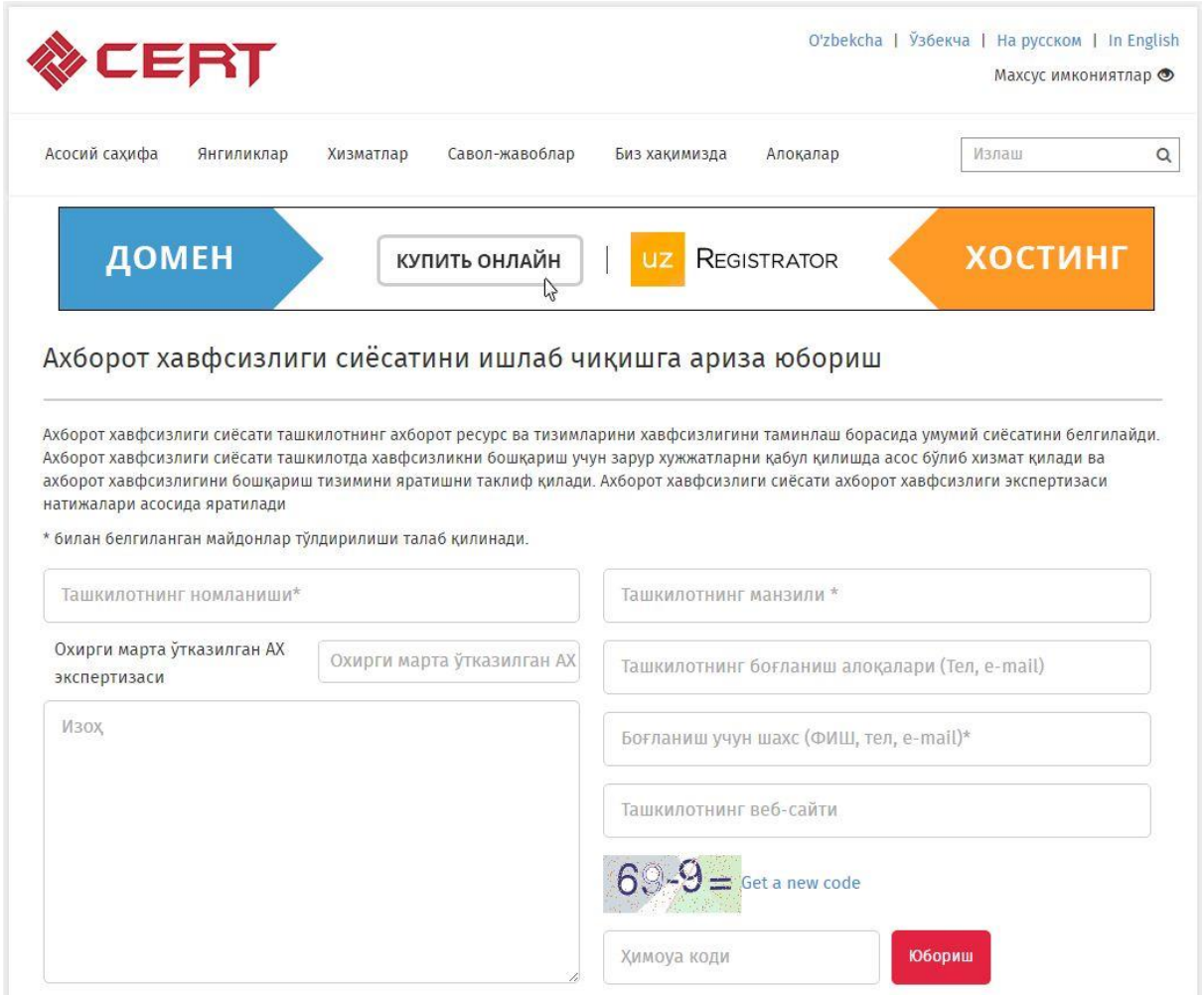
12.1-расм. UZ-CERT ташкилоти кўрсаятаётган хизматлари

Ташкилот ўз фаолияти доирасида конфиденциал маълумотлар билан ишласа (ходимлар ёки мижозлар маълумотлари) АХ экспертизасини ўтказиш ўта мухимдир. Бу турдаги маълумотларни ташқи киришлардан ҳимоялаш

шунчаки эхтиёткорлик эмас, балки ташкилотнинг асосий мажбуриятларидан биридир.

UZ-CERT мутахассислари томонидан ўтказиладиган АХ экспертизаси маълумотлар муҳимлиги даражаси, конфиденциал ахборотларни сақлаш объектларининг таҳлили ва уларни сақлаш объектларига кириш йўлларини аниқлашни, корпоратив муҳитда ечилаётган масалаларни текширишни, операцион тизим, тармоқ хизматлари протоколлари ва ҳимоя тизимлари анализини ўз ичига олади.

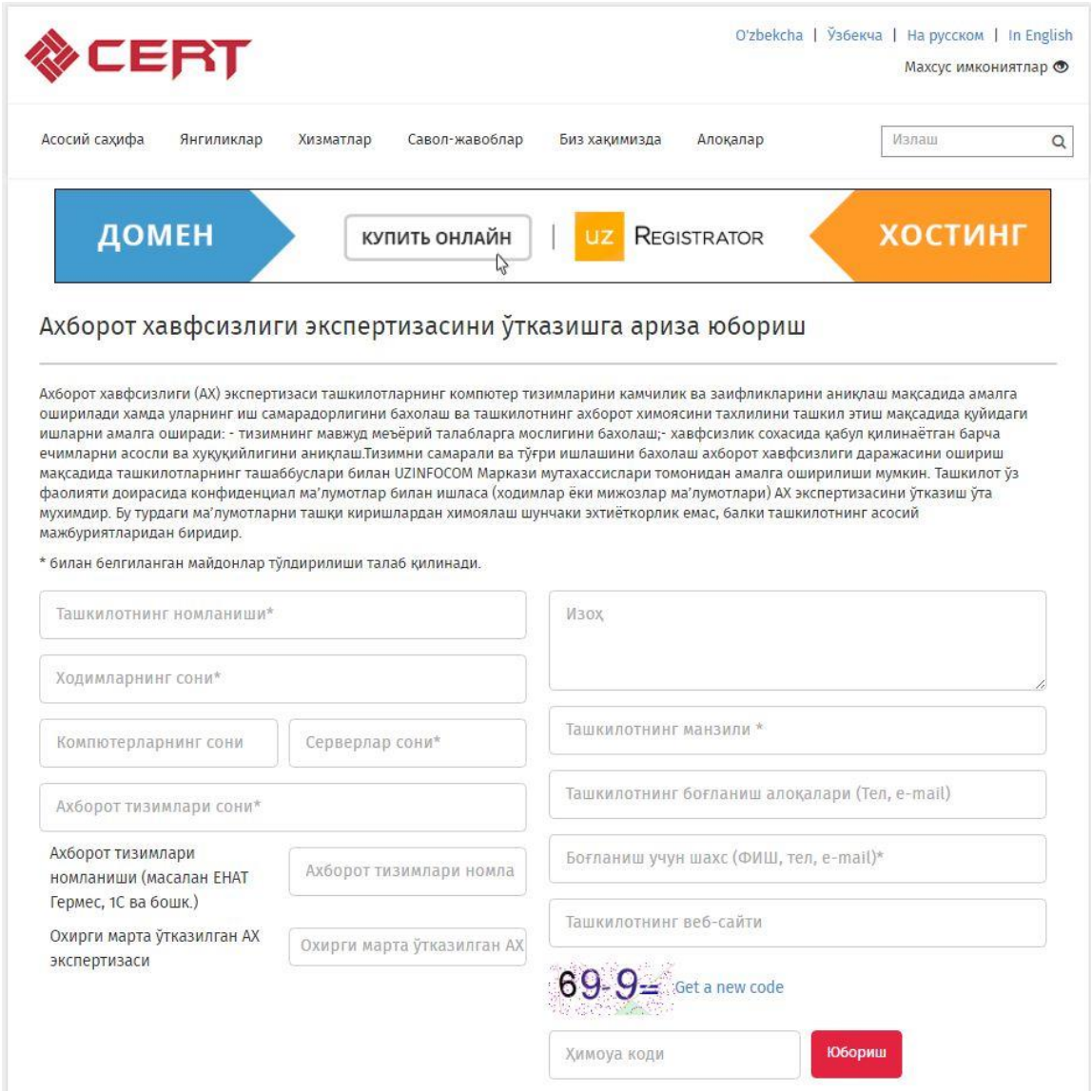
Ўтказилган, тармоқ ва тизим ахборот хавфсизлигини экспертизаси асосида, UZ-CERT мутахассислари, ташкилотнинг ахборот ресурслари ҳимоясини керакли даражага ошириш имкониятини берувчи тавсиялар берадилар.



12.2-расм. UZ-CERT ташкилоти кўрсаятаётган хизмати (АХ сиёсатини ишлаб чиқиш)

Ахборот хавфсизлиги (АХ) экспертизаси ташкилотларнинг компютер тизимларини камчилик ва заифликларини аниқлаш мақсадида амалга оширилади ҳамда уларнинг иш самарадорлигини баҳолаш ва ташкилотнинг ахборот ҳимоясини таҳлилини ташкил этиш мақсадида қуйидаги ишларни амалга оширади:

- тизимнинг мавжуд меёрий талабларга мослигини баҳолаш;
- хавфсизлик соҳасида қабул қилинаётган барча ечимларни асосли ва хуқуқийлигини аниқлаш.



12.3-расм. UZ-CERT ташкилоти кўрсаятаётган хизмати

АХ экспертизаси қуйидаги босқичлардан иборат:

- ишчи станцияларни ташқи назорати;
- серверларни ташқи назорати;

- ишчи станциялар ва серверларни локал тармоқ доирасида заифликлар мавжудлигига махсус дастурий таъминот билан сканерлаш;
- мавжуд веб-сайтларни заифликлар мавжудлигига автоматлаштирилган дастурий таъминот билан сканерлаш ва стандарт қўлости воситалари ёрдамида текшириш;
- ўрганилаётган ахборот тизими жойлашган ҳудудда мавжуд жисмоний ҳимоянинг таҳлили;
- мавжуд ички мейёрий хужжатларнининг тахлили, хусусан ахборот ҳимояси доирасида;
- ташкилотдаги жавобгар шахсларни сўровдан ўтказиш;
- оммавий ресурсларни ва тармоқда айланаётган маълумотларнинг таҳлили.

2. Америка, Европа ва Осиё давлатларида ахборот хавфсизлиги инцидентлари бўйича амалга оширилган ишлар мазмуни

Америка ва Европа мамлакатларида ахборот хавфсизлиги инцидентларини тергов қилиш етарлича ривожланган бўлиб бу борада катта ишлар ва хизматлар йўлга қўйилган.

Америка Қўшма Штатларида АХ инцидентларини тергов қилиш ва шахсий маълумотларни ҳимоялаш сервисининг бозордаги қиймати бир неча миллиард доллар қийматни ташкил этади.

Соҳанинг предмет қисми қуйидагилардан иборат:

- Инцидентларни тергов қилиш (компютер жиноятлари): ички ва ташқи инцидент, инцидент қандай содир бўлган, нима сабабли содир бўлган, айбдорлар кимлигини аниқлаш;
- Инцидентга реакция ва унинг мониторинги: инцидент содир бўлиш вақтида зарарни минималлаштириш, далилларни тўғри йиғиш ва инцидентни қандай аниқлаш;
- Компютер криминалистикаси: лоборатория компютер криминалистикаси – ҳодисалар кетма-кетлигини тиклаш, маълумот ташувчиларда далилларни қидириш, маълумотларни қайта тиклаш;

- Барча ишларни юридик олиб бориш: барча ишлар қонун доирасида олиб бориш;

RU-CERT – компютер инциденларига жавоб қайтариш маркази бўлиб, унинг асосий вазифаси – Интернетнинг Россия сегметида фойдаланувчилар учун АХ таҳдидлар содир бўлиш даражасини камайтиришдан иборат.

RU-CERT ресурсларни ёпиш, манзилларни филтрлаш, доменларни ёпиш, у ёки бу ресурс контентини ўчириш, у ёки бу ҳодисаларга алоқадор шахсларни излаш ваколатларига ега эмас.

RU-CERT инцидентга жавоб қайтариш сервисини ҳеч қандай кафолатсиз амалга оширади.

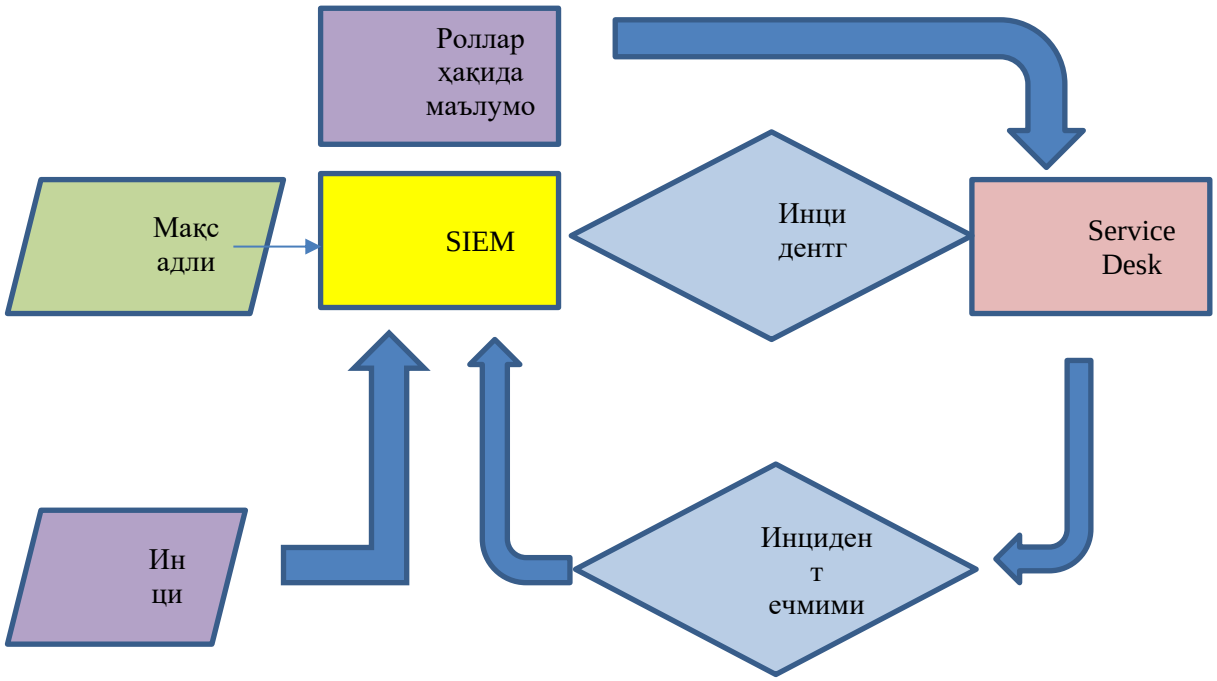
US-CERT бошқариш принципи натижасида қуйидаги вазифалар бажарилиши ва самараларга эришиши мумкин:

- Ахборотнинг юқори сифатлиги;
- Яхшиланган ахборот хабардорлиги;
- Инцидентга тезкор жавоб қайтариш.

3. Ахборот хавфсизлиги инцидентларини назорат этувчи воситалар турлари

АХ инцидентларини назорат этиш тизимлари – бу инцидентларни локализациялаш ва зарани камайтиришни таъминловчм воситалар ҳисобланади. Бу воситалар компютер инцидентлари натижасидаги зараларни камайтириш бўйича олдиндан ишлаб чиқилган автоматлаштирилган сценарийларга эга ёки масофадан ўз конфигурацияларини ўзгартириш имконияти мавжуд бўлган механизмга эга бўлади.

SIEM *(Security information and event management)* – АХни бошқариш ва хавфсизлик ҳодисаларини назорат этиш.



12.4-расм. SIEM асосидаги инцидентларни назоратлаш жараёнини автоматлаштириш тизми

АХ инцидентлари реакция ва мониторинг маркази кенг доирали АХ сервисларини тақдим этади:

АХ инцидентлари реакция ва мониторинг Маркази (SOC) дан фойдаланганда қуйидаги самараларга эришиши мумкин:

- АХ таъминлашни тайёр жараёни;
- Капитал харажатларни йўқлиги;

- Инвестиция юқорилиги;
- Сифатни ошиши;
- Инсон ресурслардан озод бўлиш.

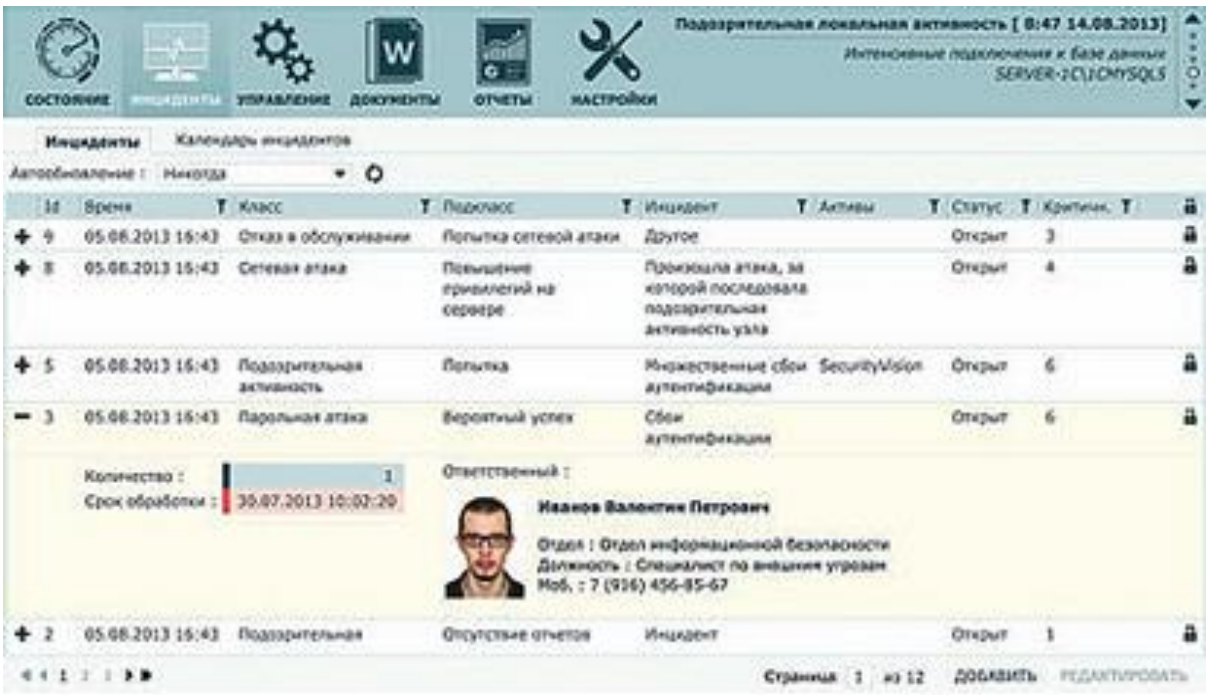
4. Ахборот хавфсизлиги инцидентларини назорат этувчи воситаларнинг тахлили

АХ инцидентларини назорат этувчи воситалар – бу тизимнинг бошқа жараёнлари билан чуқур интеграллашган тизимдир.

Инцидентларни назорат этиш воситалари амалга ошириш учун кўплаб юзага келадиган муаммоларни ечиш лозим.

Бундай тизимлар кўплаб фунцияларни ўз ичига олишини ҳисобга олган ҳолда интерфейсда намойиш этиладиган маълумотлар тўплами ҳам кенг қамровли бўлиши лозим.

12.5-расм. Инцидентларни назорат этувчи тизими интерфейига мисол



12.6-расм. Инцидентларни кузатиш ва жавобгар ходим тўғрисида маълумотни кўрсатиш

Инцидентларни назорат этиш ташкилотнинг коплекс хавфсизлигини ажралмас қисми ҳисобланади.

АХни бошқариш сиёсати таркибига жараённинг кузатиш, унга жалб этилган бўлимлар, жавобгарлар, реакция вақти, ҳисобот формалари каби маълумотлар киради.

Фойдаланилган адабиётлар

1. BS 25999-1:2006 Бизнес узлуксизлигини бошқариш – 1-қисм: Амалиёт қоидалари

2. BS ISO/IEC 27001:2005 Информацион технологиялар. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигининг бошқариш тизимлари. Талаблар

3. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

IV. АМАЛИЙ МАШҒУЛОТ МАТЕРИАЛЛАРИ

1-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги инцидентларини бошқаришни қуриш жараёнлари

Ишдан мақсад: Ахборот хавфсизлиги инцидентларини бошқариш бўйича стандартларни таҳлил этиш.

Назарий қисм: Инцидент (инцидент)- бу стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай инцидентга айтилади. (1.1-расм).

1.1-расм. Ахборот хавфсизлиги инцидентлари

Инцидентни бошқариш - бизнес жараёнларни олиб бориш жараёнида иш ҳолатини тезда минимал хавф билан нормал иш ҳолатига қайтариш фаолияти ҳисобланади, ҳамда қисқа давом этадиган ва бир мақсад сари йўналтирилган хизматлар қаторига киради.

Инцидентни бошқариш бўйича кўп стандартлар мавжуд. Улар орасидан қуйидагиларни келтириб ўтиш мумкин:

ISO/IEC 27001:2013 Information security management system. Requirements. Бу стандарт доирасида ахборот хафсизлиги тизимларини қуриш

учун умумий талаблар ва шу билан бирга инцидентлар тизимини бошқариш услублари келтирилади.

1. *ISO/IEC TR 18044 Information security incident management.* Ушбу ҳужжат PDCA циклик модели доирасида инцидентларни бошқариш инфратузилмасини таснифлайди. Ушбу стандарт ичида инцидентларни бошқариш жараёнини ташкил қилишни режалаштириш, ишга тушириш, таҳлил ва бошқа ҳолатлар тўлиқ ҳолда ҳужжатлаштириб келтирилган.

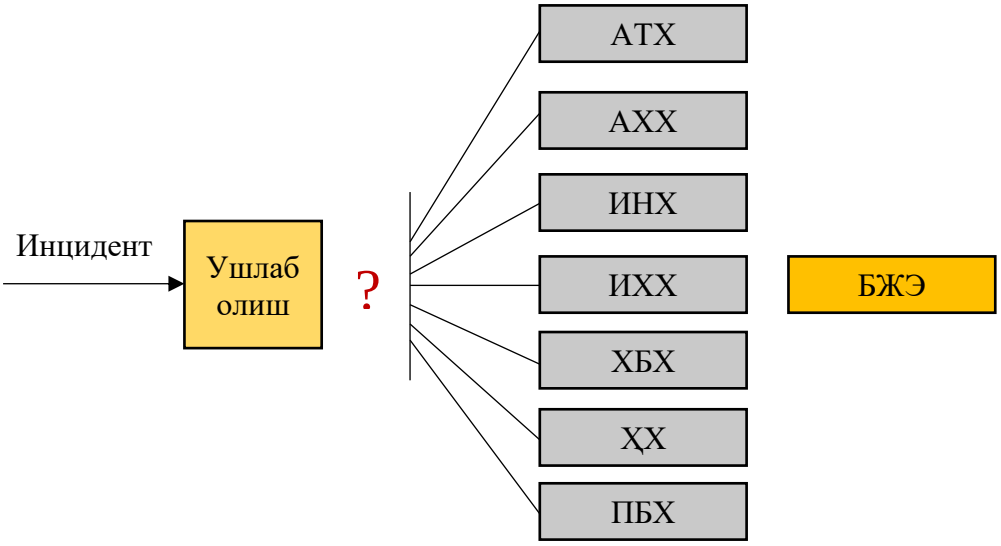
2. *CMU/SEI-2004-TR-015 Defining incident management processes for CISRT.* Ушбу ҳужжат режалаштириш, ишга тушириш жараёнининг методологияси ҳисобланади. CISRT (Critical Incident Стресс Респонсе Team). Ушбу тизимда инцидентлар юз беришини бартараф этиш, унга жавоб қайтариш ва хафсизликни таъминлаш жараёнлари асос қилиб олинади.

3. *NIST SP 800-61 Computer security incident handling guide.* Ушбу “энг яхши амалиётлар” тўплами инцидентларни бошқариш жараёнларини ташкил қилиш ва жавоб қайтариш учун қўлланма ҳисобланади. Ҳар ҳил турдаги хавфлар учун тўлақонли жавоб қайтариш ҳаракатлари ҳужжатлаштирилади.

4. *ГОСТ Р ИСО/МЭК 18044 Manaqgement information security incident.* Инцидентларни бошқариш бўйича ахборот хафсизлиги бўлими бошқарувчиларига ҳамда тармоқ мутахассисларига маслаҳатлар беради.

Муаммолар

Инцидентларни аниқлаш бу мураккаб жараёндир. Ходимлар бундай ҳолатларни билганлари учун, бундай инцидентларни олдини олишга аниқ кетма-кет ҳаракатлар қилиши зарур (1.2-расм).



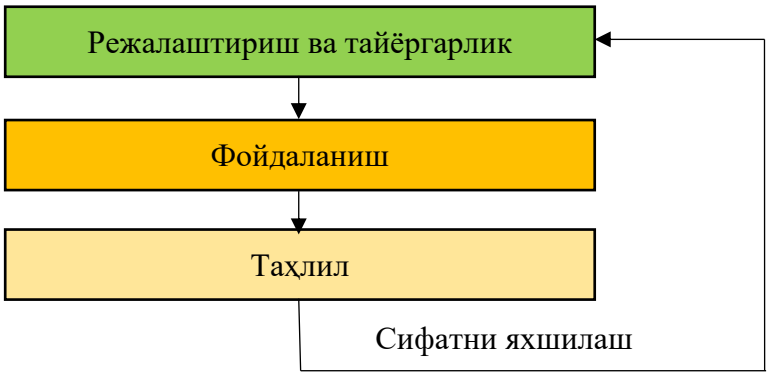
1.2-расм. Ахборот хавфсизлиги инцидентларини аниқлаш

1. Ахборот технологиялари хизмати (АТХ).
2. Ахборот хавфсизлиги хизмати(АХХ).
3. Ички назорат хизмати (ИНХ).

4. Ҳуқуқий хизмат (ҲХ).
5. Иқтисодий хавфсизлик хизмати (ИХХ).
6. Хавфларни бошқариш хизмати (ХБХ).
7. Персонални бошқариш хизмати (ПБХ).
8. Бизнес жараёнлар эгаси (БЖЭ).

Бундай ҳолатларда аниқ қандайдир кўрсатмалар ёки ходим етарлича малакага эга бўлмаса инцидентга жавоб қайтариш анча муаммоли ҳолат бўлиб чиқади. Баъзи ҳолатларда бир ходим бажариши керак бўлган ҳолатларни бир нечта ходимларга бўлиб ташланади, натижада улар параллел ҳаракат қилиб фақат вақт йўқотишади.

Келишилган ҳолатда ишлаш учун барча ходимларни аниқ ишга йўналтириш лозим 1.3-расм.



1.3-расм. Ахборот хавфсизлиги инцидентларини олидини олишни ҳужжатлаштириш

Ушбу ҳолатларни ечими қуйида 1.1-жадвалда келтирилган:

1.1-жадвал.

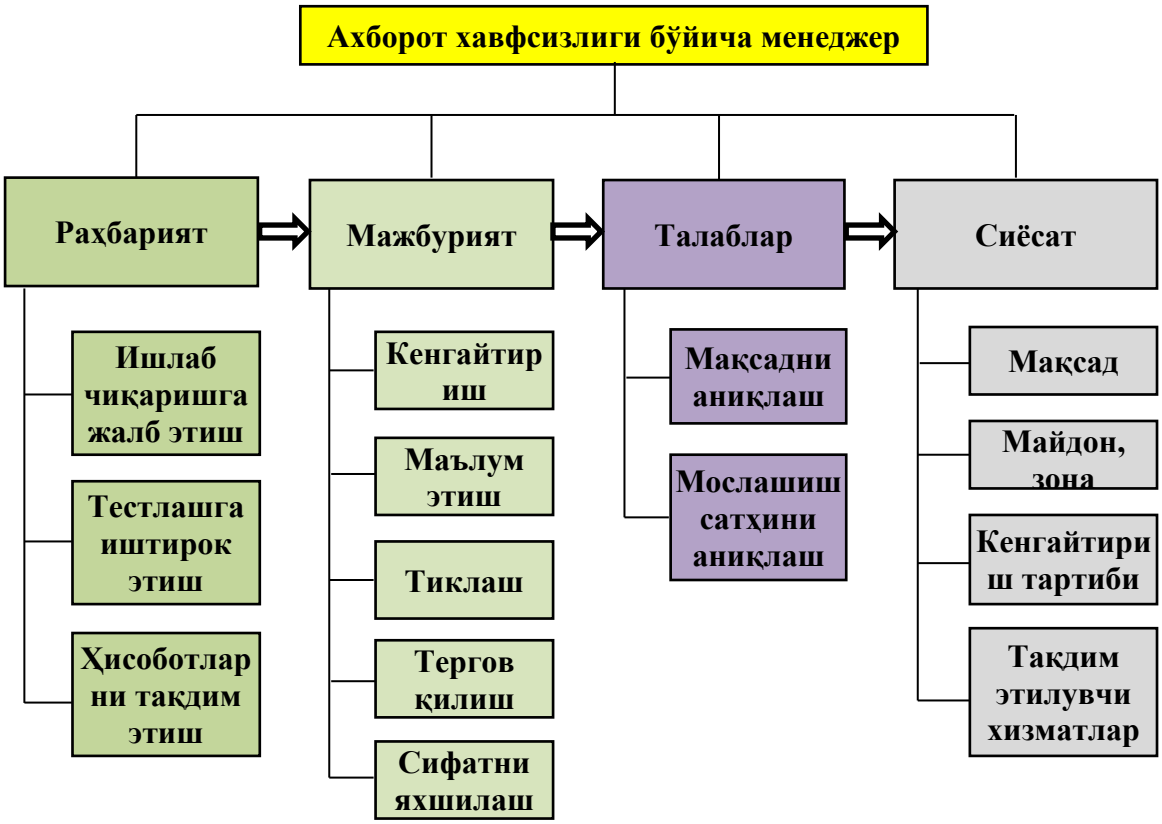
Ахборот хафсизлигидаги кутилмаган ҳолатларни олдини олиш процедураси

1.	Инцидентни тезкор аниқлаш.
2.	Инцидентни аниқ идентификациялаш.
3.	Инцидентни тўғри бошқариш.
4.	Инцидентни тўхтатиш ва камайтириш.
5.	Хизматларни тиклаш.
6.	Сабабни тушуниш.
7.	Такрорлашни бартараф этишда тадбиқ қилишни яхшилаш.

Энг аввало инцидентларни бошқариш жараёнларини бошқарувчи жавобгар шахсни аниқлаб олиш зарур. Кўп ҳолларда бу хафсизлик бўлими бошлиғи бўлади. 1.4-расмда кутиламган инцидентларни бартараф этиш бўйича асосий ечим ҳаракатлари кетма кетлиги кўрсатилган.

Талаблар ва сиёсатни ишлаб чиқиш - эксперт ечим, бу ишлаб

чиқарувчининг малакаси ва тажрибасига, ҳамда бизнес талаблар ва мақсадларга боғлиқдир.



1.4-расм. Инцидентларни бартараф этиш бўйча асосий ечимлар

Ролларни тақсимлаш - асосий ҳаракатлардан бири ҳисобланади, инцидентларни бошқариш жараёнларини қуриш тажрибасига асосан йўлларни танлаб, улар орасидан хато йўлларни ажратиш орқали амалга оширилади.

Ишни бажариш учун вазифа ва топшириқлар

1. Ахборот хавфсизлиги инцидентлари.
2. Ахборот хавфсизлиги инцидентлари мақсади.
3. Ахборот хавфсизлиги инцидентлари аниқлаш.
4. Ахборот хавфсизлиги инцидентларини бошқариш жараёнини амалга ошириш.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies,

Tools, and Techniques for Incident Analysis and Response». 2012 year.

3. David Endler, Mark Collier. Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions. McGraw-Hill/Osborne © 2007 (574 pages).

4. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

6. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью».

2-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги инцидентларини гуруҳларга ажратиш

Ишдан мақсад: Ахборот хавфсизлиги инцидентларини гуруҳларга ажратиш, хизматчи ахборотни ошкора қилиш йўллари ва активларни ўғирлашни кўриб чиқиш.

Назарий қисм: Бутун жахон тажрибасидан келиб чиққан ҳолда ахборот хафсизлиги инцидентларини ходимлар иштироки билан қуйидаги турларга бўлишимиз мумкин:

1. Ишчи маълумотларни ошкор қилиш.
2. Ҳисоботларни сохталаштириш.
3. Молиявий ёки материал активлар ўғирланиши.
4. Корхона ишига қарши бориш (саботаж).
5. Лавозимни суистеъмол қилиш.
6. Қоида бузарликни яшириш.

Ишчи маълумотларни ошкор қилиш деганда корхона ёки ушбу маълумот чиқиб кетмаслиги зарур бўлган ҳудуд доирасидан ахборотни чиқариш назарда тутилади.

Маълумотларни ошкор қилишни қуйидаги усулларини санаб ўтиш мумкин.

1. Маълумотни олиш, бундай маълумотлар кириши мумкин бўлмаган ҳудудларда ёки катта массив маълумотлар орасидан ажратиб олишга айтилади (маласан маълумотлар базасидан кўп ҳужжатларни олиш) бунда қоида бузувчи маълумотни корхонада белгиланган ҳудуддан ташқарига нусхаларда (ҳужжатларнинг ўз фото нусхаси ва ҳ.к) ёки электрон кўринишда (флеш-хотирада ва ҳ.к) ёки уларни симсиз алоқа йўли билан узатиши ҳам мумкин.

2. Маълумотларни ошкор қилиш, бунда инсайдер учинчи шахсга маслаҳат бериши мумкин. Бундай маълумот узатиш сўзлар билан гаплашиб амалга оширилиши мумкин ёки инсайдер томонидан тайёрланган ҳужжатлардан келиб чиққан ҳолда олиб борилади.

Инсайдер томонидан ишчи маълумотларни олиниши мумкин бўлган усуллар қуйидагилар бўлиши мумкин:

1. Инсайдер маълумотларни махсус тарзда қидирмайди. Унга бу маълумотлар кутилмаган тарзда қўлга тушиб қолиш сабаби ошкор қилинади, ёки бўлмаса ушбу маълумотлар унинг иш фаолияти учун зарур маълумотлар бўлиши мумкин.

2. Инсайдер ишчи маълумотларга рухсатномаси бор ва у ўзига керакли бўлган маълумотларни қидириши ёки танишиб чиқишини нусхалаши мумкин.

3. Инсайдер ишчи маълумотларга рухсатномаси йўқ, аммо унга эга бўлиш учун ўз иш фаолиятида ўзгаришларни мотивация қилиб ушбу маълумотларга

эришиш йўлларини қидириб чиқишидир.

4. Инсайдер рухсатномаси бўлмай туриб маълумотларни қўлга киритишида тизимнинг заиф жиҳатларидан фойдаланади ёки маълумотларни сақлаш қурилмасини ўғирлаш дастурлари ёрдамида олиб боради.

5. Инсайдер ахборот тизимида администратор вазифасини бажаради, алмашадиган маълумотлар бўлса унга танишув ёки нусхалаб олиш тарзида тақдим этилади.

6. Инсайдер ишчи маълумотларни бошқа ушбу маълумотларга эга инсайдер билан оғзаки сўзлашув вақтида билиб олади.

7. Инсайдер маълумотларни таҳлил қилиб ёки бошқа маълумотларни бирлаштирган тарзда топади (масалан ходимлар қандай ҳаракат қилиш ва ҳ.к.)

8. Инсайдер маълумотларга бошқа инсайдер орқали эришади, бунда иккинчи инсайдер юқорида санаб ўтилган усуллардан фойдаланган бўлиши мумкин.

9. Инсайдер томонидан ошкор қилинган маълумот юқорида санаб ўтилган усуллардан фойдаланган ҳолда қайта ишланиши мумкин.

Ҳисоботларни сохталаштириш - бу билиб туриб маълум бир ҳаракатлардан кейин маълумотларни нотўғри акс эттириш. Сохталаштириладиган ҳужжатлар корхонанинг ички ҳужжатлари ёки ташқи алоқалари ҳужжатлари бўлиши мумкин.

Мақсадга қараб ҳужжатларни сохталаштиришни қуйидаги гуруҳларга ажратишимиз мумкин:

- яшириш ёки аксинча сир сақлаш керак бўлган маълумотларни ошкор қилиш;
- асл кўрсаткичларни юқори қилиб қўйиш ёки камайтириш, шу йўл билан қўшимча даромадга эга бўлиш;
- ташкилот ходимларини хато қилишга чорлаш;
- ўзаро шартнома тузган ташкилотларни хато қилишга чорлаш.

Активларни ўғирлаш (молиявий ёки материал) - бу онгли равишда ташкилотга тегишли бўлган мол-мулкни ўзига ёки бошқа шахслар фойдасига ҳал қилиш ҳисобланади.

Материал жиҳатдан ўғирлаш қуйидаги жазо гуруҳларга бўлинади:

- ўғирлик;
- активларни ўзлаштириш ёки ишлатиб юбориш;
- ҳар хил бузғунчи йўллар билан ташкилотда асосий ёки қўшимча мақсадларга эришиш;

Бузғунчиликнинг қуйидаги усуллари кўп тарқалган:

- материал етказиб берувчилардан фойдаланиб бузғунчилик қилиш;
- мижозлар муомаласидан фойдаланиб бузғунчилик қилиш;

- кредит ёки инвестициялар бузғунчилиги;
- вексель бузғунчилик;
- банк кафолати ёки кафолат хатидан фойдаланиб бузғунчилик қилиш;
- ҳисоб рақамлари билан бузғунчилик;
- тўлов ҳужжатларини сохталаштириб ёки ўзгартириб бузғунчилик қилиш;
- пластик карталар билан бузғунчилик (сохта карталар ва операциялар);
- депозит бузғунчилиги;
- ташкилот ички мол-мулк хўжалиги фаолиятидан келиб чиққан ҳолда бузғунчилик қилиш, кўпчилик ҳолларда иш келишуви асосида.

Ташкилот ишига қарши бориш (Саботаж) - бу ташкилот фаолиятига билиб туриб қарши бориш, оқибатда ташкилот қандайдир мақсадларга эришиши имконсиз бўлади.

Ташкилот ишига қарши бориш қуйидагича гуруҳланиши мумкин:

- ташкилот обрўсини тушириш, масалан маълум бир хизматлар сифатини ёмонлаштириш ёки бошқача йўл билан зарар етказиш;
- ташкилот ходимларига нисбатан нотўғри қарорларни қабул қилиш ва шу йўл билан иш унумдорлини камайтириш;
- алоқаларни узиш, ёмонлаштириш, ёки ҳар хил усуллар билан бизнес бошқарувга тўсқинлик қилиш. Масалан, бозор шароитида рақобатчи томон ўзида устунликлар ҳосил қилиш учун шундай усуллардан фойдаланиши мумкин;
- хавфсизлик тизимларига зарар етказиш, хавфсизлик тизимларида ожиз қисмларни яратиш, бунинг натижасида ташкилот акцияларига зарар етиши мумкин;
- изларни яшириш ёки сохта изларга олиб бориш, тергов ишларини олиб бориш учун тўсқинлик қилиш;
- қимматли қоғозлар бозорида манипуляция ишларини амалга ошириш натижада негатив ҳолатни яратиш;
- ташкилотдан ёки маълум бир ходимлардан қасд олиш;
- экстремистик-террористик, сиёсий ёки шунга ўхшаш мақсадлар;
- қоидабузарликни яшириш - бу қоидабузарликни аниқлашда тўсиқ ҳосил қилиб уни яшириш ёки яширишда кўмаклашиш ҳисобланади;
- яширин қоидабузарлик ва шу билан бирга бошқа қоида бузарликлар қастдан амалга оширилиши мумкин, бунда ҳар хил ҳужжатларни сохталаштириш, маълумотларни ўчириб ташлаш ёки йўқ қилиш мумкин.

Лавозимдан ёвуз мақсадларда фойдаланиш - бу инсайдер томонидан ўз иш лавозимидан ўзига нисбатан яхши вазият яратишда фойдаланиш ҳисобланади. Ўз лавозимини суистеъмол қилишга қуйидагилар киради:

- манипуляция, хизмат кўрсатишга боғлиқ, масалан маълум бир мижозлар учун бозорда ёмон шароит яратиб ўз обрўсини ошириш;
- сотиб олиш ишлари бўйича манипуляция, маълум бир маҳсулот етказиб берувчилар учун яхшироқ шароит яратиш;
- ташкилот фаолияти орқали манипуляция.

Ишни бажариш учун вазифа ва топшириқлар

1. Ахборотни ошкор қилиш йўллари.
2. Инсайдер томонидан олинган хизматчи ахборотни ошкора қилиш йўллари.
3. Ҳисоботларни сохталаштириш усуллари.
4. Ошкор этиш усуллари.
5. Саботаж.
6. Активларни ўғирлашга қарши дастурий модуль ишлаб чиқиш.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.
3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
4. ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».

3-АМАЛИЙ МАШҒУЛОТ

Мавзу: Жараёнлар ўртасида ролларни тақсимлаш ва инцидентни бошқариш жараёнидаги ходимларни аниқлаш

Ишдан мақсад: Жараёнлар ўртасида ролларни тақсимлаш ва инцидентни бошқариш жараёнидаги ходимларни аниқлашни ўрганишдир.

Назарий қисм: Бошқарув гуруҳи томонидан қўллаб-қувватлашга эришилгандан сўнг менежмент инцидентларини бошқариш зарурлиги ва инцидентни бошқариш учун вазифаларни қандай тақсимланиши масаласини кўриб чиқишга тўғри келади. Қуйидаги жадвалда (3.1-жадвал) кўп учрайдиган лавозимлар ва у ерда рол ва қандай вазифалар бажарилиши келтирилган.

3.1-жадвал.

Вазифа ва мажбуриятлар

№	Лавозим	Вазифа	Мажбурият
1.	Ахборот хавфсизлиги маркази	Бу тузилма ахборот хавфсизлиги соҳасида тўлақонли ҳуқуқларга эга	1. Инцидентни бошқариш бўйича жавобгар. 2. Инцидентни бошқариш бўйича режа ишлаб чиқиш. 3. Истисно ва мослаштириш. 4. Охирги қарорни қабул қилиш.
2.	Ахборот хавфсизлиги бўйича менежмент	Инцидентни бошқариш гуруҳи раҳбари ва АХ маркази билан боғлаб турувчи шахс	1. Инцидентни бошқариш бўйича режаларни ишлаб чиқиш ва амалиётга тадбиқ этиш. 2. Хавфларни ва инцидентларни тўғри бошқариш. 3. Ахборот хавфини бошқаришда проактив ва актив ҳаракатларни амалга ошириш.
3.	Инцидентларда жавоб қайтариш менеджери (бази ҳолларда АХ менеджери ҳисобланади)	Инцидентларга жавоб қайтариш бўлими бошқарувчиси	1. Инцидентларга жавоб қайтариш бўлими бошқарувчилиги. 2. Ходимлар ҳаракатларини кординация қилиш. 3. Инцидентларга жавоб қайтариш режаларни муваффақиятли тугаши жавобгари. 4. АХ марказига инцидентлар ҳақида хисобот топшириш.
4.	Ахборот хавфсизлиги инцидентларига	Гуруҳ ишларида қатнашиш	1. Инцидентлар зарарини минималлаштириш. 2. Инцидентларга жавоб

	жавоб қайтариш гуруҳи аъзоси		қайтаришда кетма-кет ҳаракатларни ҳужжатлаштириб бориш. 3. Инцидент юз берганда судлашув ҳолати учун далиллар занжирини сақлаб бориш. 4. Инцидентга қандай жавоб қайтарилгани ҳақида ҳисобот ёзиб бориш.
5.	Терговчи	Кутилмаган инцидентлар гуруҳи аъзоси	1. Кутилмаган инцидент терговини олиб боради. 2. Инцидент сабабини аниқлайди. 3. Тергов ҳақида хисобот тайёрлайди.
6.	АХ бўйича АТ мутахасис	Ахборот хавфсизлиги инцидентларига жавоб берувчи гуруҳ аъзоси.	1. Инцидентда терговни амалга ошириш. 2. Хавфсизликни таъминлаш учун қўшимча чора-тадбирларни амалга ошириш.
7.	Бизнес бўлим бошқарувчиси	Бизнес жараён ва активлар эгаси	1. Жараён/ресурс/тизим ҳақида инцидентлар гуруҳи маслаҳатларидан келиб чиққан ҳолда қарорлар қабул қилиш. 2. Активларни тиклашни аниқлаш ва бизнес жараёнларда таҳдидларни баҳолашини ўтказиш.
8.	АТ мутахассис	АТ бўлими ходими	1. Инцидентларни йўқотиш жараёнида ахборот хавфсизлиги инцидентларига жавоб берувчи гуруҳ аъзосига ёрдам бериш. 2. Тасдиқланган қоида ва сиёсат асосида корхона ахборот тизимини қўлаб-қувватлаш.
9.	Ҳуқуқшунос	Ҳуқуқлар бўлими ходими	Бошқариш/жавоб қайтариш/тергов вақтида ёрдам беради.

10.	Кадрлар бўлими ҳодими	Ходимларни бошқариш бўлими мутахассиси	1. Бошқариш/жавоб қайтариш/тергов вақтида ҳодимдан шубҳа қилинса ёрдам беради. 2. Инцидентни бошқаришга тегишли аспектларни бошқариш сиёсатини қуриш.
11.	Пресс-котиб (а)	Оммавий ахборот воситалари билан ишлаш мутахассиси	Брендларни сақлашни ва корхона обрўсини, ОАВ ни, ва акционерлар инцидентини сақлаш мақсадида ахборот тақдим этиш.
12.	Хавфларни таҳлил этувчи мутахассис	АХ бўлими ходими, хавфлар бўйича ички бошқарув ёки хавфларни бошқариш	1. Хавфларни камайтириш ва уларни бошқариш учун бўлим бошлиқлари билан бирга ишлаш. 2. Асосий маълумотларни тақдим этиш (хавфларни бошқариш стратегияси).

Асосий калит вазифаларини аниқлаб олганимиздан сўнг, инцидентларни бошқариш жараёнини ҳужжатлаштириш керак бўлади.

Исталган жараёндаги каби инцидентларни бошқариш ҳам жараёни циклик равишда доимо ривожланиб бориши зарур. (3.1-расм).

3.1-расм. Тестлаш ва яхшилаш

Исталган жараённи бошқаришда шу жараённинг қийин нуқталари мавжуд бўлади. Ушбу муаммоларни ҳал қилиш эса ишнинг қанчалик унумдор бўлишини аниқлаб беради. Тажрибадан келиб чиққан ҳолда қуйидаги

муаммоларни ажратиб олдик (3.2-расм).

3.2-расм. Ахборот хавфсизлиги инцидентларини бошқаришда юзага келадиган муаммолар

Инцидентларни бошқариш қийин жараён ҳисобланиб, ҳодимлардан бирга ва аниқ ишлашни талаб қилади. Ҳар қандай инцидент жуда катта муаммога айланиб кетмаслиги учун олдиндан белгиланган қоидаларга тўлақонли амал қилиш зарур бўлади.

Жараён тўғри бориши 90% ҳодимларга боғлиқ бўлгани учун асосий эътиборни кутиламган инцидентларга қандай жавоб қайтариш ва иш фаолиятини қандай тиклаш режаларини ташкил қилиш масаласига қаратиш лозим.

Инцидент қуйидаги қоидаларга амал қилиши лозим:

- ходимлар ва меҳмонлар хавфсизлиги;
- инцидентни минимал зарар билан ушлаб туриш;
- ташкилот активлари хавфсизлиги;
- ахборот технологиялари хавфсизлиги;
- бизнес талабларидан келиб чиқиб ишни тиклаш;
- инцидент тергови;
- шундай инцидент қайта такрорланмаслиги учун чора-тадбирлар.

Ушбу қоидалар ахборот хавфсизлиги инцидентлари жараёнини самарали бошқаришни қуришга амалий ёрдам беради.

Ишни бажариш учун вазифа ва топшириқлар

1. Ахборот хавфсизлиги инцидентларини жавоб қайтариш гуруҳи.
2. Ахборот хавфсизлиги инцидентларини тестлаш ва яхшилаш.
3. Ахборот хавфсизлиги инцидентларини бошқаришдаги муаммолар.

4. Ахборот хавфсизлиги инцидентлари қоидалари.

Фойдаланилган адабиётлар

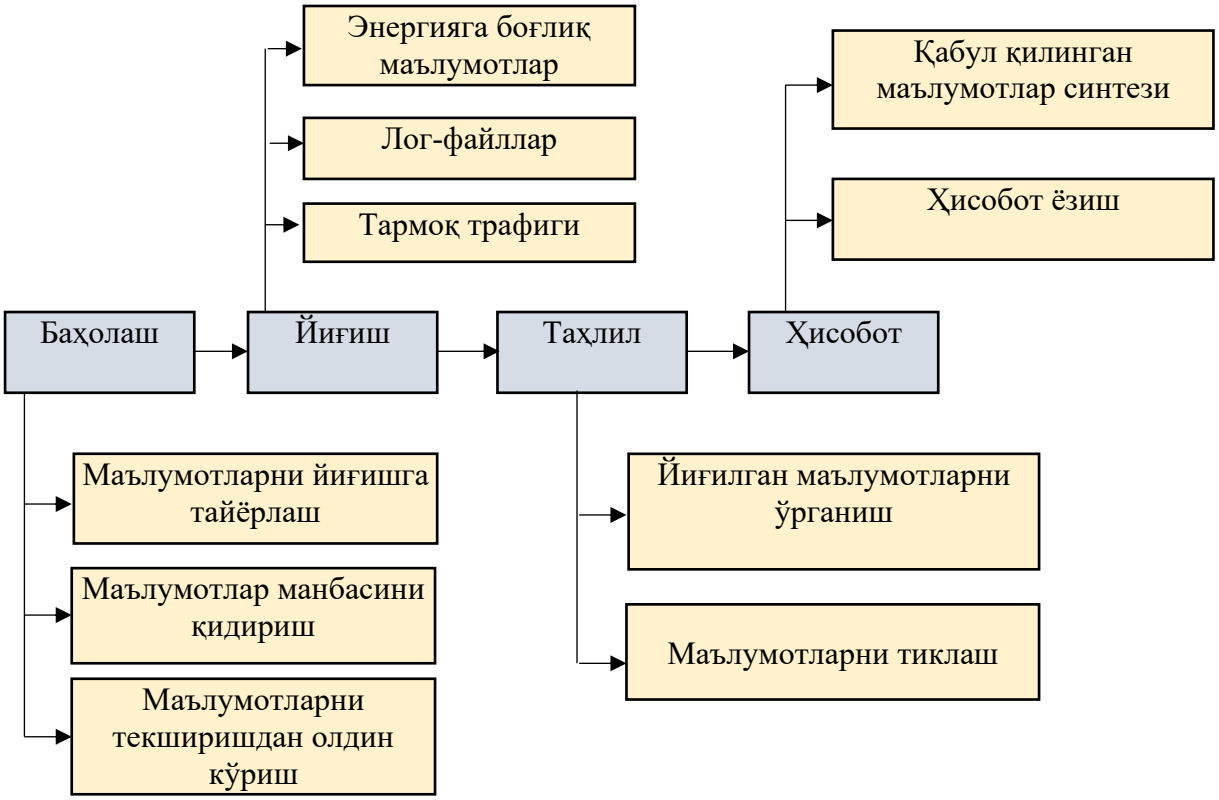
1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.
3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
4. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».
5. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». – М.: Стандартинформ, 2009. – 50 с.
6. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».

4-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги инцидентларининг тергови

Ишдан мақсад: Ахборот хавфсизлиги инцидентлари терговини ташкил қилишни усул ва воситаларидан фойдаланиш.

Назарий қисм: Инцидентлар тергови энг аввало ахборот хавфсизлигида тергов жараёни қандай ташкил қилинишини кўриши лозим. Умумий ҳолатда бу қуйидагича акс эттириш мумкин: (4.1-расм).



4.1-расм. Ахборот хафсизлигида инсидентларни тергов қилиш

1 даража: Баҳолаш. Бу даражада маълумотларни йиғишда тайёргарлик ишлари бошланади, тергов амалга ошириш мумкинлиги аниқланади (тергов ўтказиш учун рухсатнома олинади, терговнинг қонунга тўғри келиши аниқланади); тергов ўтказадиган гуруҳ аъзолари аниқланади; гуруҳ инцидент бўлган тармоқ топологиясини ўрганади ва ҳ.к.

Шу билан бирга баҳолаш жараёнида инцедентга боғлиқ бўлиши мумкин бўлган компютерлар тузилмаси ҳам ўрганиб чиқилади.

2 даража: Йиғиш. Бу даражада инцидентга тегишли деб ҳисобланган барча маълумотлар йиғилади. Улар ўз ичига:

- энергияга муҳтож маълумот сақлаш қурилмаларини ўрганиб чиқиш (қаттиқ дисклар);
- энергияга муҳтож қурилмаларни сақлаш (оператив хотира);
- тармоқ қурилмалари лог-файллари;
- тармоқ трафиги.

Юқорида санаб ўтилганлардан маълумотларни нусхалаб олишдан фойдаланиш мумкин.

Энергияга муҳтож қурилмалар тузилмаси. Энергияга муҳтож қурилма нусхасини олишдан олдин маълумотлар бутунлигини (ўзгармаганлигини) текшириб олиш зарур, яъни бу дастурий ёки қурилмали нусхалашдан ҳимоялашда ишлатилади. Агар компьютерга ахборот сақлаш қурилмаси ўрнатилган ва уни нусхалаб олиш керак бўлса энг аввало ушбу компьютер иши тўхтатилади ва шундан сўнг энергияга муҳтож ахборот сақлаш қурилмаларини нусхалашни бошлаш мумкин.

Ёзишдан ҳимоялаш қурилмалари ўрганиладиган ахборот сақлаш қурилмасини ёзилишдан олдин хавфсиз равишда кўчириб олиш имконини беради. Қурилмали ёзишдан сақлаш жиҳозлари эса дастурий таъминотларга боғлиқ бўлмаган ҳолда ўз вазифасини бажаришда давом этади. Кўпчилик ҳолларда ёзишдан ҳимоялаш қурилма кўринишида эмас дастур кўринишида келади, маълум бир операцион тизим ичида келади ва LiveCD ёки флеш хотира орқали асосий тизим билан бирга юкланади. Бундай операцион тизимларга қуйидагиларни мисол қилиб келтириш мумкин:

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

Нусхалаш учун қуйидаги дастурлардан фойдаланиш мумкин:

- dd (Linux барча дистрибутивлари ичида бор);
- dc3dd- модификацияланган версияси dd;
- aimage;
- FTK Imager.

Маълумотларни ўрганиб чиқишдан олдин нусхалаш мажбурий қадамлардан бири ҳисобланмайди. Агар маълумотнинг асл нусхаси бошқа жойда сақланса ва кимдир унинг нусхаси билан ишлайдиган бўлса уни яна бир марта нусхалаш бу ортиқча ҳаракат ҳисобланади. Ишлаб турган тизимларда энергияга муҳтож маълумотларни йиғиш уларни ўчиришдан олдин амалга ошириалди. Кўпчилик ҳолларда қуйидаги энергияга муҳтож маълумотлар сақлаш блоклари нусхалаб олинади:

1. Оператив хотирадаги маълумотлар.
2. Мониторланадиган, шифрланган ва ҳамда тармоқ сақлаш қисмлари.
3. Ишлаб турган процессорлар қисмлари.
4. Мавжуд бўлган тармоқ уланишлари ва портлар.
5. Ўрганилаётган тизим тармоқ тузилмаси.
6. Атрофдаги ўзгарувчилар.

7. Фойдаланувчилар экранда кўрадиган расм.

Бу маълумотларни нусхалаш учун ўрганилаётган тизимга махсус маълумот ташиш қурилмалари уланади, унинг ичидан эса дастур ишга тушади ва маълумотларни йиғишни бошлайди. Баъзида бундай дастурлар тармоқ орқали ҳам юкланиши мумкин. Нусхаланган маълумотлар ташқи хотирада сақланиши ёки тармоқ орқали узатилиши мумкин.

Лог-файллар. Логларни нусхалаш бир нечта усул билан амалга оширилиши мумкин:

- фақат ёзувларни нусхалаш билан (масалан маълум бир IP-адресга га тегишли бўлган);
- лог-файлларни тўлақонли нусхалаш;
- маълумотларни сақлаш қурилмасини тўлақонли нусхалаш.

Қайси усулда нусхалашни танлашда асосий фактор бу: лог-файлларнинг ишончлилиги, изланишлар доираси, лог-файлларнинг ўзгариш даражаси ва ҳажмига қаралади. Бошқа ҳолларда маълумот сақлаш қурилмасини тўлақонли нусхалаган фойдалидир.

Тармоқ трафиги. Тармоқ пакетларидан (dump) нусха олиш учун қуйидаги дастурлардан фойдаланиш мумкин:

- tcpdump;
- Wireshark.

Бунинг учун тармоққа уланиш талаб қилинади ва тармоқнинг бу қисмидан криминалистика учун керак бўладиган барча пакетлар ўтиши талаб қилинади. Бундай нусхалаш пайтида dump нусхаланиш вақтини камайтириши керак бўлади.

3 даража: Таҳлил. Бу даражада барча йиғилган маълумотлар таҳлил қилинади ва бунда қуйидаги алгоритмлардан фойдаланилади:

- ўрганилаётган объект ҳақида тўлиқ маълумот йиғилади (дисклардан, dumpдан, тармоқ трафигидан ва ҳ.к.);
- маълумотларни шаффофлигини таъминлаб бериш;
- маълумотларни яширин тарзда ўрганиб чиқиш (шифрланган маълумотларни ўрганиш);
- энергияга муҳтож маълумотлар сақлаш қурилмаларини ўрганиб чиқиш ва қайта тиклаш.

Криминалистик изланиш деганда йўқолган ёки ўчириб ташланган маълумотларни излари орқали қидириб топиш назарда тутилади. Бундай излар ахборот тизимларида жуда кўп бўлади, оддийгина белгилашлардан, ўзгаришлардан, виртуал хотира фрагментларидан, MAC адреслардан мослаб танланади.

Криминалистик изланишлар учун қуйидаги дастурлардан фойдаланиш

мумкин:

- EnCase Forensic;
- Forensic Toolkit;
- The Sleuth Kit.

Қайта тиклаш учун эса қуйидаги дастурлардан фойдаланилади:

- Foremost;
- PhotoRec.

Тармоқ dump хотирасини таҳлил этиш учун ишлатиши мумкин бўлган дастурлар:

1. Тармоқ пакети турини аниқлаш учун (масалан ёпиқ файлларни қидириш учун).
2. Тармоқ орқали юбориладиган хабарларни очиб кўриш учун.

Биринчи ҳолатда қуйидаги дастурлар ёрдам беради:

- Wireshark;
- Network Miner.

Иккинчи ҳолатда эса тармоқ анализатор дастурлари эмас, пакетларни ушлаб олиш тизимларидан фойдаланишга тўғри келади. Бундай қидирув маълум бир калит сўзлар орқали қидиришга айтилади.

4 даража: Ҳисобот. Бу даражада таҳлил натижасидан олинган барча маълумотлар синтези амалга оширилади ва шу маълумотлардан келиб чиққан ҳолда ҳисобот ёзилади, ҳисобот ўз навбатида қуйидагиларни ўз ичига олиши зарур:

- инцидент юз беришига нима сабаб бўлгани;
- инцидентга алоқадор шахслар;
- инцидент қандай давом этгани;
- аниқланган излар тўлиқ тарзда тушунтириб берилгани;
- тергов жараёнида ишлатилган усуллар, дастурлар ва қурилмалар ҳақида тушунчалар ва уларни кейинчалик қаерда қўллаш мумкинлиги ҳақида маслаҳат;
- бундай инцидентларни олдини олиш бўйича маслаҳат.

Ишни бажариш учун вазифа ва топшириқлар

1. Инцидентларни тергов этиш.
2. Лог-файллар
3. Тармоқ трафиги.
4. Тармоқ трафигини таҳлил этувчи дастурий модуль ишлаб чиқиш.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной

информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.

2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.

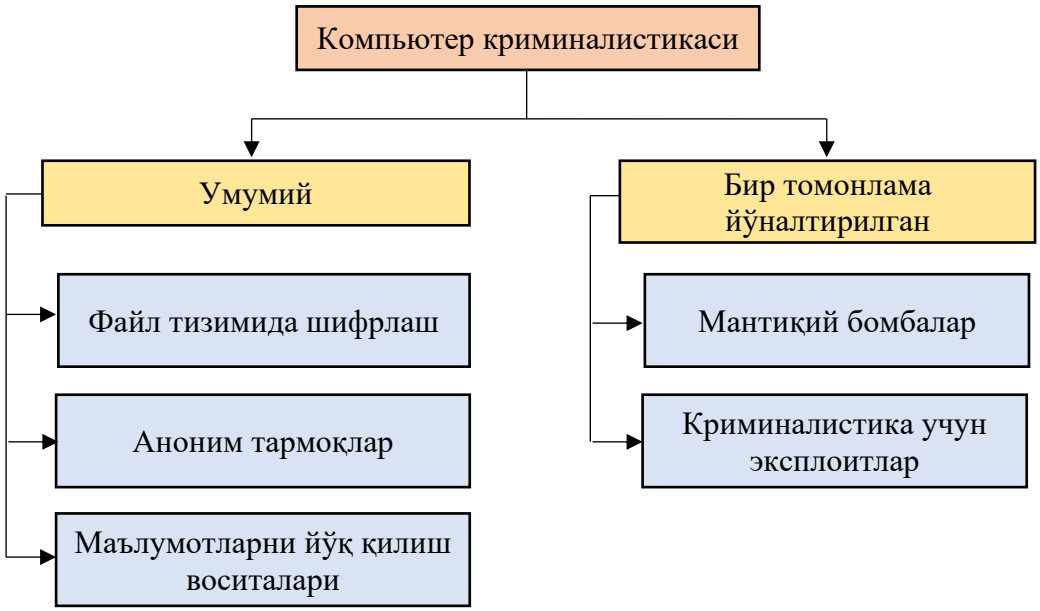
3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

5-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги инцидентларини тергов қилиш жараёнидаги қаршиликлар

Ишдан мақсад: Ахборот хавфсизлиги инцидентларини тергов қилиш жараёнидаги юзага келадиган қаршиликлар ва уларни ечиш усулларини ўрганиш.

Назарий қисм: Ахборот хавфсизлиги инцидентларини тергов қилиш даражасида бузғунчи томонидан қаршиликларга учраш мумкин. Бундай ҳаракат бир томонлама йўналтирилган ёки умумий бўлиши мумкин (5.1-расм).



5.1-расм. Компьютер криминалистикаси

Умумий қарши ҳаракатлар. Умумий қарши харакатлар кимгадир ёки нимагадир йўналтирилмаган бўлиб кўпчилик ҳолларда икки хил вазифани бажарувчи ресурслардан фойдаланилади (мисол, файл тизими шифрлашини яратувчи дастурлар ёки тармоқ трафигини шифрловчи дастурлар). Ушбу қарши ҳаракатнинг асосий мақсади маълумотларни шифрлаш, йўқ қилиш ёки яшириш йўллари билан криминалистик тадқиқотлардан ҳимоя қилишдир.

Йўналтирилган қарши ҳаракат ёки криминалистик ҳаракатни алдаш, ушбу ҳаракатнинг асосий йўналишларидан бири ҳисобланади. Ушбу турнинг асосий мақсади: криминалистик изланишлардан маълумотларни сақлаш, криминалистик усуллар ишончсизлигини кўрсатишдир.

Ушбу ҳаракатнинг бошқа турида криминалистик текширув олиб бораётган ташкилот тармоғига рухсатсиз кириб маълумотларга ўзгартириш киритишдан иборат ҳисобланади (бунинг учун дастурлар ва қурилмаларнинг заиф қисмларидан фойдаланилади). Энг кўп тарқалган усуллардан бири бу умумий қаршилик ҳаракатлари ҳисобланади. Мақсадга йўналтирилган қарши ҳаракатлар кам ўрганилган бўлим ҳисобланади.

Қаршилик ҳаракатларининг умумий усуллари. Энг кўп тарқалган қаршилик ҳаракатларидан бири бу- маълумотларни ҳимоялаш бу-шифралаш, стенографик яшириш, қайта ёзиш ёки ўчириб ташлаш ҳисобланади.

Шу билан бирга ҳозирги кунда криминалистик изланишларда мумкин бўлган маълумотларни йўқ қилишга қаратилган усуллар ҳам кўпдир. Бундай дастурлар оператив хотирада ишлайди. Бундай усуллар ва дастурлар кўп ҳолларда шахсий маълумотларни конфиденциал(махфий) сақлаш учун ёки сўз эркинлигини сақлаб қолиш учун ишлатилади.

Юқорида санаб ўтилган усуллар қўлланилиши кибержиноятни очиш учун катта тўсиқ ҳисобланади, аммо бир қанча криминалистик усуллар мавжудки улар шундай ҳимояланган маълумотларни топиш ва очиш учун мўжалланган ҳисобланади.

Инцидентларни терговга қарши мақсадга йўналтирилган усуллар. Мақсадга йўналтирилган усуллар криминалистик қийматга эга бўлган маълумотларни аниқлаш ва уларни йўқ қилишдан иборат ҳисобланади. Криминалистик терговни аниқлаш эса бир қанча усуллардан фойдаланган ҳолда амалга оширилиши мумкин: тармоқ воситаларини ишлаш аломатларини қидириш мақсадида тармоқ трафигини таҳлили, ишлаётган дастурлар таҳлили ва ҳ.к.

Бир томонлама йўналтирилган ҳаракатлар. Маълумотларни йўқ қилиш, яшириш ёки ўзгартириб қўйиш мантиқий бомбалардан ёки криминалистик дастурларга қарши эксплоитлардан фойдаланишлар орқали амалга оширилади(бундай воситалар дастур хатоликларидан фойдаланиши мумкин).

Йўналтирилган қаршилик кўрсатиш асосан криминалистиканинг қуйидаги заиф жойларига ҳужум қилиши мумкин:

4. Усул.
5. Восита.
6. Ҳаракат.

Усул - компьютер маълумотларини ўрганиб чиқиш учун умумий усуллар. Масалан: криминалистик операцион тизим юкланиши, у ўз навбатида нусхалашдан ҳимояланмаган тарзда ишга туширилади, кейинчалик керакли файллардан нусха олиш учун ҳам ишлатилади.

Восита - дастур ёки қурилма ҳисобланиб, криминалистик изланишларнинг маълум даражасида фойдаланилади. Мисол: Криминалистик Live CD grml.

Ҳаракат - маълум бир даражадаги мақсадга йўналтирилган ҳаракатлар кетма кетлигидир. Масалан: файлларни нусхалаш учун дастур ишга туширилиши (натижа: дискда мавжуд бўлган файллар нусхаланиши)

файлларни индекслаш учун дастурни ишга тушириш (натижа керакли файлни калит сўзлар ёрдамида тездо топиб олиш).

Юқорида келтирилган заиф нуқталарга қарши қуйидаги ҳаракатларни келтиришимиз мумкин:

4. Карши ҳаракат қурилмада махсус файллар яратиш орқали: криминалистик изланиш аниқланса дархол файлни алмаштириб қўйиш.

5. Дастурий воситалар ёрдамида қаршилик кўрсатиш.

6. Криминалистик изланиш олиб борилгани ҳақида факт маълум бўлгач криминалистик ишлаётган дастурлар турларини аниқлаш.

Аппарат(ёрлиқлар). Кўпчилик криминалистик ҳаракатларга қарши қўллаш мумкин бўлган усуллардан бири аппарат ёрлиқлар ҳисобланади. Маласан, криминалистик изланишлар олиб борилиши аниқлангандан сўнг файлга ўзгартиришлар киритиш ёки йўқ қилиш бу аппарат ичига киритилган ёрлиқ ҳисобланади. Бундай услуб билан Live CD ёки дастурий модуллардан қутилиш учун фойдаланиш мумкин. Бошқа мисол эса маълумотларни аппаратли йўқ қилиш ҳисобланади. Бунда кутилмаган тарзда маълумот сақлаш қурилмасини очишга уринишдир. Бундай ҳолатларда батарея ишга тушади ва узоқ вақт давомида кучли ток билан таъсир ўтказади.

Дастурий (ёрлиқлар). Яқин кунларгача дастурий ёрлиқлар фақатгина баъзи ҳолларда ўзини яхши кўрсата олар эди. Масалан Live CD дискка ёзишдан ҳимояланмаган ҳолда компьютерни ишга тушириши мумкин. Хозирги кунда эса улар маълум бир криминалистик изланишларга ҳам қарши тура оладиган дастурий восита сифатида фойдаланилмоқда.

Ишни бажариш учун вазифа ва топшириқлар

1. Компьютер криминалистикасини тадқиқ этиш.
2. Инцидентларни тадқиқ қилишдаги қарши ҳаракатларнинг умумий усуллари.
3. Аппарат «ёрлиқлар».
4. Дастурий «ёрлиқлар».
5. Компьютер криминалистикасида ишлатиладиган дастурий воситаларни созлаш усуллари.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.

2. Савельева М.В., Смушкин А.Б. Криминалистика. Учебник. М,: Издательство Издательский дом «Дашков и К». - 2009 г. - 608 ISBN: 978-5-

91131-836-9.

3. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. - М.: «Логос», 2012.

4. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».

5. NIST SP 800-61 «Computer security incident handling guide».

6-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги инцидентлари терговида гуруҳлар тузилмаси

Ишдан мақсад: Ахборот хавфсизлиги инцидентлари терговида гуруҳлар тузилмаси билан ишлаш ва инцидентларни бартараф этишда гурух тузилмаси моделларини таҳлил этиш.

Назарий қисм: Инцидентларга жавоб қайтариш гуруҳи ташкилотнинг исталган ходими учун очиқ бўлиши лозим. Инцидентни тергов этиш қанчалик мураккаблигига қараб унда бир ёки бир нечта иштирокчилар қатнашиши мумкин. Жамоа раҳбари инцидент гувоҳларини таҳлил қилади ва гуруҳда нечта ва қандай йўналишдаги ҳодимлар бўлиши кераклиги ҳақида қарор қабул қилади.

Жавоб қайтариш гуруҳининг тузилмасини уч хил модели мавжуд:

Марказлаштирилган модел – бутун ташкилот доирасида ягона тизим тарзида ташкил қилинган модел бўлиб, у уч бўлимдан иборат бўлади: call center (телефон қўнғироқларига жавоб маркази), техник ёрдам маркази (маълумотларни йиғиш ва таҳлил қилиш маркази), тергов қилиш гуруҳи (аналитик марказ). Ушбу модел унча катта бўлмаган ташкилотлар учун мўлжалланган.

Тақсимланган модел – марказлаштирилган модел асосида яратилган. Ушбу моделнинг марказлаштирилган моделдан фарқи ташкилот филиаллари географик узоқликда жойлашганлигидадир. Ушбу ҳолатда асосий офиснинг жавоб қайтариш гуруҳи ахборот хавфсизлиги инцидентлари ҳақида мувофиқлаштириш хизмати ва маълумотларни сақлаш билан тўлдирилади.

Корпоратив модел – соҳага оид марказий принципга асосан амалга оширилади. Мувофиқлаштириш бўлими инцидентга жавоб қайтариш саволлари бўйича юридик шахслардан керакли маълумотларни олади, шу билан бирга унинг қарамоғидаги ташкилотларни ҳам бошқаради.

Жавоб қайтариш гуруҳи ҳодимлари уч асосий модел остида йиғилиши мумкин:

- ташкилот вужудга келган инцидентни қайта ишлаш бўйича барча вазифани ўз зиммасига олади ва ўз ходимларига таянади;
- жамоа таркибига ушбу соҳа вакилларидан аъзолар қабул қилинади. Ушбу модел ўз ресурсларига 24/7 схемаси остида ишлайдиган ташкилотларга тўғри келади. Бундай ҳолатда жавоб қайтариш ва қайта ишлаш масаласини фирма ўз зиммасига олади, тергов ишлари билан эса ташкилот ичидаги гуруҳ шуғулланади;
- инцидентга жавоб қайтариш ва уни қайта ишлаш ишлари тўлақонли бошқа ташкилот ёки фирмага юкаланади. Бу модел ташкилотни қўлидан қайта

ишлаш имконияти келмайдиган тақдирдагина қўлланилиши мумкин.

Моделни танлашдаги факторлар:

1. Ахборот тизими доим 24 соат ҳафтасига 7 кун мавжудлиги.

2. Тўлақонли ёки қисман ходимлар бандлиги. Ушбу факторга агар ходимлар тўлақонли банд бўлмасагина аҳамият бериш мумкин. Ходимлар билан кутилмаган ҳолларда боғланиш йўлларини кўриб чиқиш лозим.

3. Ходимлар маҳорати. Ахборот хафсизлиги инцидентларини қайта ишлаш ахборот хавфсизлигини махсус дастурий-аппарат воситаларини билиши талаб этади. Ташкилот ишчи йўллашдан олдин ушбу жиҳатни эътиборга олиши лозим.

4. Ахборот хафсизлиги инцидентларини бошқаришни нархи. Ташкилот ахборот хафсизлиги инцидентларини бошқариш нархини баҳолаши ва ўзи учун фойдали моделни аниқлаб олиши керак.

5. Ташкилий тузилма. Фақат инцидентларни қайта ишлашда корпоратив ёндашувдан фойдаланган ҳолда ахборот хафсизлиги инцидентларини тергов этишда эркин ҳаракат қила оладиган жамоалар тузиш мумкин. Бунда энг яхши ечим марказий офисда мувофиқлашган марказ ташкил этиш бўлади.

Ташқаридан хизмат кўрсатиш факторлари:

1. Кўрсатилган хизмат сифатига жавобгарлик. Ташкилот бошқа фирма томонидан бажариладиган ишнинг сифатини текшириб боради. Шунинг учун ахборот хафсизлиги мониторингини юритиш талаб этилади.

2. Маъмурлик ваколатларини ажратиш. Қурилмани ўчириб ёқиш бўйича даража, фойдаланувчилар ҳақидаги маълумотлар ўзгариши ҳамда бошқа ҳаракатлар инцидент юз берганда кечадиган жараёнлар олдиндан келишиб олиниши ва ҳужжатлаштирилиши лозим.

3. Ахборотга рухсатни чеклаб қўйиш. Ташкилот ахборот махфийлиги ҳимоясини кўриб чиқади. Умумий ҳолда бошқа фирма бизни ташкилот тузилмасини тўлақонли ўрганиб чиқишига имконият яратиб бермаслик керак (ходимлар ҳақида малумот, иш ёзишмалари, ҳужжатларни сақлаш каталоги ва бошқалар).

4. Ташкилот тузилмасини билиш. Ташкилот ҳизмат кўрсатувчи фирмага ўзи ҳақида тўғри тасаввур яратиш учун ҳаракат қилиши зарур. Ташкилот инцидент қандай юзага келган бўлиши мумкинлиги ҳақидаги ҳужжатни яратади ва ҳар доим уни такомиллаштириб бориши лозим.

5. Юзага келган инцидент коррелцияси. Ташкилот ахборот хафсизлиги инциденти юзага келганда ушбу вазиятни коррелациялаш тизимини ишга тушириши керак. Ушбу тизим махсус билимни талаб қилади;

6. Инцидентларни қайта ишлаш. Ташкилот ҳизмат кўрсатиш фирмаси ходимини инцидентни тергов этиш жараёнида иштирок этиши ёки

этмаслигини аниқлайди.

7. Инцидентларга мустақил равишда жавоб қайтара олиш. Ташкилот ахборот хафсизлигида юзага келадиган инцидентларда мустақил равишда жавоб қайтаришни билиши керак. Инцидент кўпайиши билан хизмат кўрсатувчи фирма билан алоқа узилиб қолиши мумкин. Бундай ҳолатлар учун ташкилот авариявий режасини ишлаб чиқиши керак.

Ташкилот тузилмалари билан алоқа

Молиявий ташкилот танланган моделидан қатъий назар энг камида иккита ахборот хафсизлигига жавоб бера оладиган ҳодимга эга бўлиши зарур. Ушбу ҳодимлар кутилмаган инцидент юз берган вақти муаммони ўзлари бартараф қилишилари ёки ҳизмат кўрсатиш ташкилотлари билан боғланишлари керак бўлади. Ходимлар малакасига қараб юзага келган инцидент тез ва кам чиқим билан бартараф этилиши лозим.

Инцидентни қайта ишлаш жараёнида ташкилот жавоб қайтариш гуруҳига нисбатан қуйидаги сиёсатни қўллаши лозим:

- инцидентларни қайта ишлашни молиялаштириш тартиби;
- жавоб қайтариш гуруҳи ходимларини бошқа йўналишларда малакасини ошириш;
- норматив ва техник ҳужжатларни ёзишда жавоб қайтариш гуруҳи азоларини ҳам бириктириш;
- жамоа маркази тўлиқ бирлашган бўлиши лозим ва ҳамма ўз вазифасини тўлиқ билиши шарт;
- ишчилар ротацияси амалиёти доим қўллаб қуватланиши керак;
- инцидентлар юзага келганда ўзини қандай тутиши кераклиги ҳақида курслар ташкил қилиш ва тестлар олиб бориш;
- инцидент юзага келган ҳолатларда бошқа йўналишдаги ходимларни ҳам жалб қилиш. Масалан юрист, АТ муҳандиси, ҳодимлар билан ишлаш бўлими ва бошқалар.

Ишни бажариш учун вазифа ва топшириқлар

1. Ташкилот ёки муассасада ахборот хавфсизлиги инцидентларни бартараф этиш моделлари.
2. Ташқаридан ҳизмат кўрсатишни ёллаш факторлари.
3. Жавоб қайтариш гуруҳига сиёсатни.
4. Ташкилот ёки муассасада ахборот хавфсизлиги инцидентларини бартараф этишда ишчи гуруҳи структураси ва алгоритмини ишлаб чиқиш.
5. Ташкилот ёки муассасада ахборот хавфсизлиги инцидентларини бартараф этиш ишчи гуруҳни ишлаш принципларини мувофиқлаштирувчи дастурий маҳсулот ишлаб чиқиш.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.
3. David Endler, Mark Collier. Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions. McGraw-Hill/Osborne © 2007 (574 pages).
4. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

7-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хафсизлиги инцидентларига жавоб қайтаришнинг асосий босқичлари

Ишдан мақсад: Ахборот хафсизлиги инцидентларига жавоб қайтаришнинг асосий босқичларини ўрганиш ва уларни қўллаш усуллари.

Назарий қисм: Ахборот хафсизлигида инцидент юзага келишида кўп ҳолларда комплекс ва кўп томонлама муаммолар сабаб бўлади. Ушбу муаммонинг тўғри ечими биринчи навбатда уни структура компоненталарига декомпозиция қилиш ва ҳар бир компонент учун кирувчи ва чиқувчи маълумотларни ўрганиб чиқишдир.

Инцидентга жавоб қайтаришнинг асосий босқичлари қуйидагилар:

1. Инцидент юзага келишига тайёр бўлиш. Ташкилот инцидент юзага келиш ҳолатига тайёр бўлиши лозим (унинг оқибатларини камайтириш учун).
2. Инцидентларни ўрганиб чиқиш бўйича комиссия тузиш (CSIRT). Бу босқич муҳим босқичлардан бири ҳисобланади ва ҳамда инцидентни тергов қилишни муваффақиятли ўтиши ҳам бу босқичга боғлиқдир.
3. Инцидентни аниқлаш - ахборот хафсизлиги инцидентини идентификацияси.
4. Бошланғич жавоб қайтариш - биринчи даражали тергов ишларини бошланиши, асосий воқеаларни ёзиб олиш, комиссия тузилиш, тергов олиб борилишига алоқадор шахслар аниқланиш. Қонунга хилоф ҳаракатларни аниқлаш.
5. Жавоб қайтариш стратегиясини шакллантириш. Стратегия маълум бўлган барча фактларга асосланиб қурилади. Компаниянинг топ-менеджери томонидан тасдиқланади. Стратегия шу билан бирга қандай ҳаракатлар амалга оширилиши кераклигини ҳам кўрсатиб ўтади.
6. Инцидент тергови - маълумотларни таҳлили ва йиғиши орқали олиб борилади. Барча тўпланган маълумотлар ўрганиб чиқиб қачон бўлган, қаерда бўлган, ким томондан қилинган ҳаракатлар текширилади.
7. Ҳисобот - тўлақонли ҳисобот ўз таркибида тергов давомида топилган маълумотлар бир жойга йиғилиб тушунарли тарзда баён қилинганлиги ҳақида маълумот беради.
8. Ечим - ҳимоя механизмларини ташкил қилиш ва кейинчалик бундай вазиятлар бўлишини олдини олиш.

Бўлиши мумкин бўлган инцидентлар. Ҳар бир инцидент бошқасидан фарқ қилади ва ўзгача ечим талаб қилиши мумкин. Шунинг учун ишчи гуруҳ ҳар бир ҳолатга ҳар ҳил ёндашиши керак. Бўлиши мумкин бўлган инцидентлар:

1. Серверни бузиш.

2. Электрон пулларни ўғирлаш.
3. IP-телефонияни бузиш.
4. Тармоқ трафиги ўғирлаш.
5. Махфий маълумотларни чиқиб кетиши.
6. Маълумотлар йўқолиши.
7. Мақсадга йўналтирилган вирусли ҳужумлар.
8. Бошқа инцидентлар.

Тезкор тарзда инцидентга жавоб қайтариш бу қисқа вақт ичида режа ишлаб чиқиб инцидентни бартараф этиш назарда тутади. Мутахассислар инцидентни омадли бартараф этиш учун қуйидаги ишларни амалга оширишади:

- 24/7 режимида мутахассислар маслаҳати;
- тезкор тарзда инцидентни бартараф этиш режасини ишлаб чиқиш ва ёрдам бериш;
- мутахассисга талаб;
- тезкор тарзда катта хавфларни бартараф этиш;
- криминалистик экспертизани амалга ошириш;
- зараркунанда дастурларни тадқиқ қилиш (вируслар);
- маълумотларни тиклаш;
- бажарилган ишларни юридик жиҳатдан кузатиб бориш, керакли ҳужжатларни тайёрлаш ва ҳуқуқни сақлаш органларига тақдим этиш;
- ахборотни ҳимоялашни яхшилаш бўйича тавсиялар бериш;
- инцидентни ўрганиб чиқишда режа ишлаб чиқиш ва тавсиялар бериш.

Ишни бажариш учун вазифа ва топшириқлар

1. Жавоб қайтариш стратегиясини таснифи.
2. Махфий маълумотларни йўқолиб қолишини таҳлил этиш ва уларга қарши кураш .
3. Мақсадга йўналтирилган вирусли ҳужумлар.
4. Дастурий модуль ишлаб чиқиш.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.
3. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

4. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». – М.: Стандартинформ, 2009. – 50 с.

5. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».

6. NIST SP 800-61 «Computer security incident handling guide».

8-АМАЛИЙ МАШҒУЛОТ

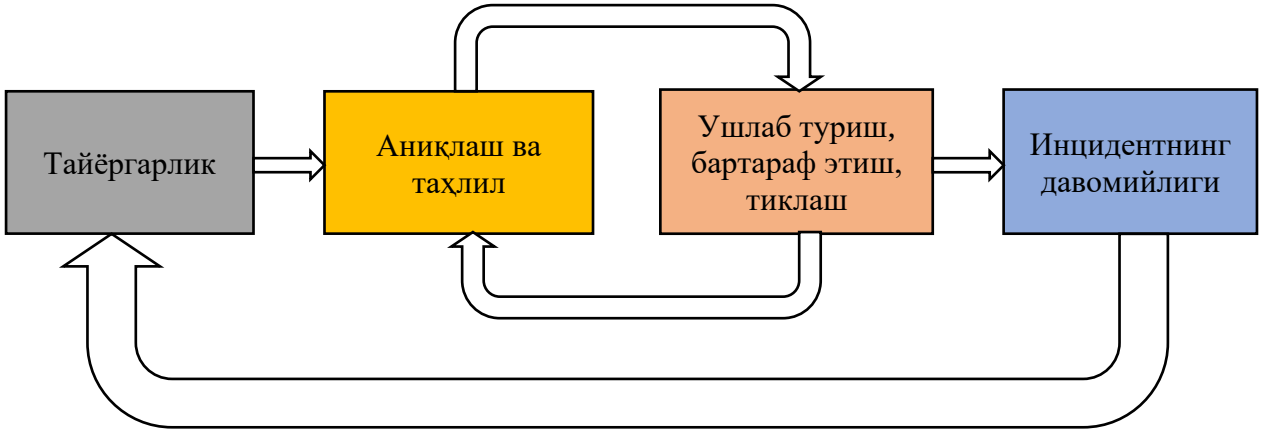
Мавзу: Ахборот хавфсизлиги инцидентларига жавоб қайтариш процедурасининг ҳаётий даври

Ишдан мақсад: Ахборот хавфсизлиги инцидентларига жавоб қайтариш процедураси ҳаётий даврини таҳлил этиш.

Назарий қисм: Ахборот хафсизлиги инцидентларига жавоб қайтариш процедураси бир нечта босқичлардан таркиб топган. Ходимларни ўқитишдан бошлаб махсус қурилмалар ва инцидентлардан чиқиб кетишгача бўлган вақтни ўз ичига олади. Ташкилот бундай инцидентларга тайёргарлик қилиш вақтида ҳар доим кутилмаган инцидентлар сонини камайтиришга интилади.

Кўпчилик ташкилотлар бундай ҳолларда ахборот хафсизлиги менежметини қўллашади бу эса оз навбатида кутилмаган инцидентларни ўрганишини соддалаштиради.

Ахборот хафсизлигини таминловчи механизмларни ишга тушириш ва ташкил қилиш анча катта меҳнатни талаб қилади ва алоҳида ҳизмат корсатиш керак бўлади. Инцидентларга жавоб қайтариш қуйидаги даражаларни ўз ичига олади: тайёргарлик, аниқлаш ва таҳлил, ушлаб туриш/бартараф қилиш/қайта тиклаш инцидентдан кейинги босқичлар. Инцидентларга жавоб қайтаришни ҳаётий даври қуйидаги 8.1-расмда келтирилган.



8.1-расм. Инцидентларга жавоб қайтаришни ҳаётий даври

1. Тайёргарлик

Инцидентларга ҳар ҳил услублар билан тайёргарлик кўриш, бу фақатгина инцидентларга тайёр туриш эмас, шу билан бирга уларни олдини олиш ахборот хафсизлигини яхшилаш ҳам саналади.

1.1. Инцидентларни қайта ишлаш

Қуйида кутилмаган инцидентларни қайта ишлаш учун мавжуд бўлган қурилмалар ва ресурслар келтирилади. Масалан смартфонлар иш ҳаракатни кординациялаш учун яхши ечим ҳисобланади. Ташкилот алоқа қилиш ва иш ҳаракатларни бошқариш учун бир қанча ечимларга эга бўлиши зарур.

Жавоб қайтариш гуруҳи аъзолари боғланиш услублари:

1. Боғланиш учун манзиллар гуруҳ доирасида ёки ташқарисида,яъни ташкилот ичидан чиқмасдан.
2. Инцидент эслокацияси ҳақида маълумот.
3. Ҳисобот механизми.
4. Муаммоларни бошқариш тизимида инцидент ҳақида малумотарни қидириш ва бошқалар.
5. Шифрлаш учун дастурий таъминот, гуруҳ аъзолари ўртасида алоқа ўрнатиш учун ишлатилади.

Инцидентни таҳлил қилиш учун қурилма ва дастурий таминот:

1. Махсус ишчи стол криминалистик ишларни амалга ошириш учун дискларни нусхалаш, файл журналларини олиш ва бошқа амалларда фойдаланилади.
2. Ноутбуклар махсус ташкил қилинадиган йиғилишлар учун ишлатилади.
3. Захиравий ишчи станциялари ва серверлари, тармоқ қурилмалари. Шу билан бирга уларга эквивалент ҳисобланадиган ҳар қандай қурилмалар.
4. Хотира қурилмалари.
5. Принтер, файл журналлар ва бошқа керакли бўлган далилларни чиқариш учун.
6. Пакет ва протоколлар анализатори трафикни йиғиш ва таҳлил қилиш учун.
7. Криминалистик дастурий таъминот дискларни таҳлил қилиш ва йиғиш учун.
8. Далилларни йиғиш учун бошқа қурилмлар, масалан камера, диктофон ва стикер ва бош.

Инцидентни таҳлил этиш учун ресурслар:

1. Портлар рўйхати, кўп ишлатиладиган портлар ҳақида маълумот.
2. Ташкилотда фойдаланиладиган ОТ дастурлари ва протоколлари ҳақида ҳужжатлар.
3. Тармоқ схемаси.
4. Тармоқ ва дастурлар тўғри ишлаши.
5. Текширув суммалари.

Инцидентдан кейинги жараённи тиклаш:

1. Автоматлаштирлган образларга рухсат.

2. Аниқлаш ва анализ

2.1. Хужум йўналишлари. Ҳужум йўналишлари бу шундай тушунчаки унинг ичида ҳужум қилиниши мумкин бўлган умумий услублар келтирилади ва улар қуйидагилардир:

1. Ташқи хотира қурилмалари.

2. Тизим унумдорлигини пасайиши.
3. Web дастурлар.
4. Электрон почта.
5. Рухсатсиз фойдаланиш.
6. Қурилмалар йўқолиши ёки ўғирланиши.

2.2. Инцидент аломатлари. Инцидент аломатлари икки турга бўлинади: бўлиши мумкин инцидентлар ёки индикаторлар. Бўлиши мумкин бўлган инцидентлар келажакда бўлиш эхтимоли бор инцидентлардир. Индикатор эса инцидент бўлиб ўтгани ёки ҳозирда бўлаётганини англатади.

2.3. Бўлиши мумкин бўлган инцидентлар ва индикаторлар манбалари.

- кутилмаган киришларни олдини олиш, бартараф этиш;
- хафсизлик жараёнларини бошқариш;
- зарарли дастурлардан ҳимоя қилиш ва анти спам дастурлари;
- файллар бутунлигини текширувчи дастур;
- мониторинг ҳизматлари.

Жараёнларни ёзиш журнали:

- операцион тизим ва дастурлар;
- тармоқ қурилмалари;
- очиқ ҳолда мавжуд бўлган янги заиф томонлар, ҳамда эксплойтлар.

Одамлар:

- ташкилот ходимлари.

2.4. Инцидент таҳлили. Қуйида инцидент таҳлилини соддалаштириш учун маслаҳатлар келтирилган:

- тизим ва тармоқни индекслаш;
- журналларни сақлаш сиёсатини яратиш;
- инцидентлар корреляциясини амалга ошириш;
- тизимда бир хил вақт бўлишини кузатиб бориш;
- изланишлар учун интернетда қидирув тизимларидан фойдаланиш;
- қўшимча маълумотлар олиш учун снифферлардан фойдаланиш;
- маълумотларни филтрлаш;
- экспертлардан ёрдам сўраш.

2.5. Инцидентни ҳужжатлаштириш. Инцидентни ҳужжатлаштиришда қуйидагиларни ҳисобга олиш зарур ҳисобланади:

- инцидентнинг ҳозирги аҳволи;
- инцидент ҳақида қисқача тушунча;
- инцидентга боғлиқ индикаторлар;
- ушбу инцидентга боғлиқ бошқа инцидентлар;
- инцидентни қайта ишлашда қатнашаётган ҳодимлар иш ҳаракати;

- далилларни йиғиш, рўйхатдан ўтказиш ва сақлашда жавобгарлик;
- зарарни баҳолаш;
- инцидентга боғлиқ томонларнинг манзиллари;
- тергов жараёнида аниқланган далиллар рўйхати;
- инцидентни қайта ишлашини шархлаш;
- инцидент тугагандан кейин қандай ҳаракат қилиш кераклигини аниқлаш.

2.6. Инцидентларни даражаланиши. Инцидентларни даражалаш бу энг муҳим босқич ҳисобланади. Чекланган имкониятларда энг катта зарар етиши мумкин бўлган қисмни аниқлаш ва бартараф қилиш жуда қулай ҳисобланади. Шунинг учун ҳам инцидентларни гуруҳлаш талаб қилинади.

Инцидентнинг функционал таъсири:

- мавжуд бўлмаган - ходимлар ва ташкилотга ҳеч қандай зарар етгани йўқ;
- паст даражали - ташкилот барча сўнги хизматларни кўрсатиши мумкин, аммо пасайган самара билан;
- ўртача - ташкилот баъзи фойдаланувчилар учун хизмат кўрсата олмай қолади;
- юқори - ташкилот жуда муҳим бўлган баъзи хизматларни кўрсатмайди.

Инцидентга ахборот таъсир ўтказиш:

- таъсир йўқ - ҳеч қандай маълумот ўзгартирилмаган, ўчирилмаган ёки бирлаштирилмаган;
- конфиденциалликни бузилиши – ташкилотда конфиденциал ахборотларни ўғирланганлиги;
- бутунлик йўқотилиши - конфиденциал маълумотлар ўзгартирилса ёки йўқ қилинса.

Инцидентдан кейинги ҳолат:

- доимий - кайта тиклаш учун вақт ва ресурслар етарли;
- вақтинчалик - қайта тиклаш учун вақт етарли лекин қўшимча ресурслар талаб қилинади;
- кенгайтирилган - қайта тикланиш учун вақт аниқмас; ҳар томондан ёрдам керак бўлади;
- тиклаш мумкин эмас -инцидентдан кейин тиклаш мумкин эмас, тергов этиш керак.

2.7. Инцидент ҳақида ҳақида огоҳлантириш. Инцидент таҳлил қилиб даражага ажратилганидан кейин, жавоб қайтариш гуруҳи жавобгар шахсларга мурожат қилиши зарур.

Инцидентдан келиб чиққан ҳолда қуйидаги шахсларга мурожат қилиш мумкин:

- ахборот технологиялари бошлиғига;
- хафсизлик бўйича бошлиғига;
- ташкилот ичидаги инцидентларга жавоб қайтариш гуруҳларига;
- инцидентларга жавоб қайтаришнинг ташқи гуруҳларига;
- тизим эгасига;
- ишчилар бўлимига;
- ҳуқуқшуносга;
- хонани ҳимоя қилувчи шахсларга.

Инцидент ҳақида огоҳлантириш учун қуйидаги алоқа воситаларидан фойдаланиш мумкин:

- электрон почта;
- web сайт;
- телефон қўнғроқ;
- овозли почта;
- қоғозда ёзилган хат.

3. Ушлаб туриш, бартараф этиш ва тиклаш

3.1. Ушлаб туриш стратегиясини танлаш. Ушлаб туриш стратегияси инцидент турига қараб ҳар хил бўлиши мумкин. Масалан, почтага вирусли хат келган ҳолат билан DDOS ҳужум бир-бири билан катта фарқ қилади. Ташкилот ҳар қандай ҳолатлар учун алоҳида стратегия ишлаб чиқишига тўғри келади. Стратегия эса ўз навбатида қуйидагиларни ўз ичига олиши зарур:

- ресурсларни бузиш ёки ўғирлаш;
- далилларни сақлаб қолиш;
- хизматлар мавжудлиги;
- стратегияни амалга ошириш учун керак бўладиган вақт ва ресурслар;
- стратегия унумдорлиги;
- давомийлик.

3.2. Далилларни йиғиш ва қайта ишлаш. Ҳар қандай далил учун деталли маълумотларни сақлаш керак ва улар қуйидагиларни ўз ичига олиши зарур:

- идентификацияланадиган маълумот (масалан IP-адрес , MAC адрес ва бошқалар);
- инцидент билан ишлаган ҳар бир одамнинг Ф.И.О., лавозими ва телефон номери;
- вақт;
- сақлаш жойи.

3.3. Ҳужум қилувчининг идентификацияси. Ҳужум қилаётган шахсни аниқлаш учун қилинадиган амаллар қуйида келтирилган:

- қидирув тизимлари орқали ҳужум қилаётган шахсни қидириш;

- ички ёки ташқи маълумотлар базасидан фойдаланиш;
- ҳужум қилиниши мумкин бўлган каналлар мониторинги.

3.4 Ҳужумларни бартараф этиш ёки қайта тиклаш. Инцидентни аниқлаб уни тўхтатишга эришилгандан кейин у етказган зарарни қайта тиклашга тўгри келади. Баъзи инцидентлар учун қайта тиклаш жараёни қийин бўлмайди.

Қайта тиклаш ҳолати маълум дастур ёки ОТ туридан келиб чиққан ҳолда ҳар хил бўлиши мумкин.

4. Инцидентнингдавомийлиги

4.1. Ўрганилган дарслар. Инцидентнинг кўриб чиқиш қисмида қуйидагиларни аҳамиятга олиш зарур:

- нима болди ва қандай вақтда?
- ходим ёки жавобгар шахс ишни қай даражада бажара олди?
- хужжатлаштириш жараёни амалга оширилдими? Жараёнларни анализ қилиш шартми?
- қандай маълумот олдин керак бўлган?
- бундай ҳолатларни олдини олиш учун нималар қилиш зарур?
- ташқи томонлар билан алоқани яхшиласа бўладими?
- қандай ҳаракатлар бундай ҳолатларни олдини олади?
- худди шундай инцидентларни аниқлаш учун қандай қўшимча ресурс ёки қурилмалар керак болади?

4.2. Инцидент асосидан йиғилган маълумотларни қайта ишланиши. Ўлчаш лозим бўлган бирликлар:

- қайта ишланган инцидентлар;
- ҳар бир инцидент учун йўқотилган вақт бирлиги;
- ҳар бир инцидентни қайта ишлаш унумдорлиги;
- ҳар бир инцидентни субъектли баҳоланиши.

Инцидентларни аниқлашда аудит сиёсати. Аудит мавжуд бўлган муаммоларни кўрсатиб беради ва кейинчалик уни бартараф этиши мумкин бўлади. Энг кам ҳолатда аудит қуйидаги саволларга жавоб бериши зарур:

- инцидентга жавоб қайтариш сиёсати режаси ва жараёнлари;
- ресурс ва фойдаланиладиган қуроллар;
- жамоанинг тузилмаси ва модели;
- инцидентни қайта ишлаш жараёнида иштирок этган шахсларни қайта ўқитиш ва малакасини ошириш;
- инцидент ҳақида ҳужжарлар;
- инцидентни бошқариш унумдорлигини баҳолаш.

Ишни бажариш учун вазифа ва топшириқлар

1. Ахборот хавфсизлиги инцидентларига жавоб қайтариш процедурасининг ҳаётий даври нечта фазани ўз ичига олади?

2. Инцидентларга жавоб қайтариш ҳаёт даврини тушинтириб беринг?

3. Тайёргарлик фазасида нималар амалга оширилади?

4. Ушлаб туриш, бартараф этиш ва тиклаш фазасини амалий таҳлил қилинг.

5. Инцидентдан кейинги давомийлик жараёнида нималар амалга оширилади?

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.

2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.

3. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

4. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

5. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».

6. NIST SP 800-61 «Computer security incident handling guide».

9-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги инцидентларига жавоб қайтариш алгоритми

Ишдан мақсад: Ахборот хавфсизлиги инцидентларига жавоб қайтариш алгоритмини тадқиқ этиш ва ундан фойдаланиш усуллари.

Назарий қисм: Ҳозирги кунда банкларнинг асосий эътибори ахборот хавфсизлиги инцидентини бошқаришга қаратилган. Бунинг асосий сабабларидан бири масофавий банк тизимларида ўғирликлар содир этилиши кўпайиб кетгани сабаб бўлмоқда. Ахборот хавфсизлиги инцидентлари банк фаолиятидаги бизнес жараёнлар бузилишига, иқтисодий мавқеъга ва ишончни йўқотишга жиддий таъсир ўтказиши мумкин. Ва ҳатто ахборот хавфсизлигидаги кичкина муаммоалар ҳам йиғилиб катта бузилишга олиб келиши мумкин. Ахборот хавфсизлиги инцидентларини бошқариш тизимидан фойдаланиш ва тадқиқ этиш банк ҳодимлари иш жараёнларини бошқариш учун имкониятлар яратиб беради. Шуни асосида етказиладиган зарар камаяди, тезда вазиятни бартараф этиш имкони бўлади.

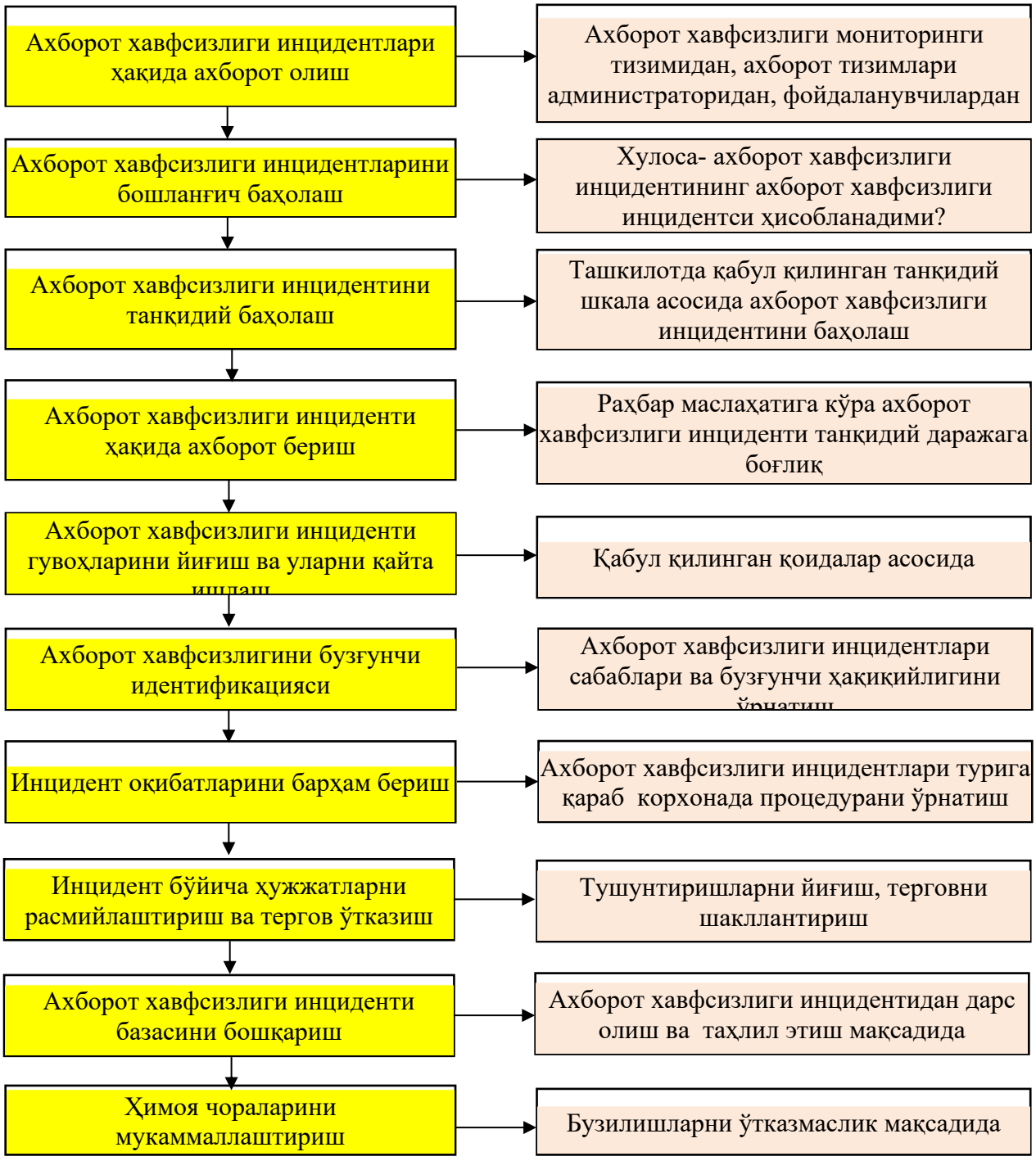
Ўз вақтида инцидентларни аниқлаш, уни пайдо бўлишига жавоб қайтариш ва кейинчалик такрорланмаслигини кўриб чиқиш керак. Ҳозирги кунда шунақа стандартлардан бири бу ГОСТ Р ИСО/МЭК ТО 18044-2007 стандарти «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» (ГОСТ 18044-2007)- ахборот хавфсизлиги инцидентларига бағишланган асосий стандартлардан бири ҳисобланади. Ахборот хавфсизлиги инцидентларига тайёргарлик, тезкорлик кўп ҳолларда етказиладиган зарар камайишига имкон беради. Кўп инцидентлар вақт ўтиши билан пайдо бўлади, бунинг оқибатида ҳар хил ёмон оқибатлар юзага келади, шунинг учун ҳам ахборот хавфсизлиги хизматларининг асосий вазифаларидан бири шундай оқибатларни тезда аниқлашдир.

Тўғри тузилган ва режалаштирилган инцидентларни бошқарув усулида (ГОСТ 18044-2007 стандарти) қуйидагиларни келтириш мумкин:

- оптимал усуллар асосида ахборот хавфсизлиги инцидентлари идентификациясига рухсат бериш ва баҳолаш;
- ҳимоя чораларига мос равишда ахборот хавфсизлиги инцидентлари салбий оқибатлари таъсирини камайтириш;
- ахборот хавфсизлиги инцидентларидан тўғри дарс олиш.

Жавоб қайтариш алгоритми. Барча керакли жараёнларни ишга туширгандан кейин, банк тизими режали ва тизимли текширувлар ўтказиб бориши зарур. Шу йўл билан ахборот хафсизлиги инцидентларини аниқлаш осонлашади. Умумий ҳолда инцидентларни аниқлаш ва уларга жавоб

қайтаришни қуйидаги алгоритмда кўриш мумкин: (9.1-расм).



9.1-расм. Ахборот хавфсизлиги инцидентларида жавоб қайтариш ва уларни аниқлаш алгоритми

Ахборот хавфсизлиги инцидентларида жавоб қайтариш процедураси инцидент турига, унинг танқидий даражасига, бўлиши мумкин бўлган зарарларига, ташкилот раҳбарияти жавобига қараб турли хил бўлиши мумкин. Ҳозирги кунда ахборот хавфсизлиги инцидентларига катта эътибор қаратилмоқда. Табиий равишда, ҳозирда бир қанча банклар молиявий йўқотишларга дучор бўлмоқда. Фактларни пайдо бўлиш ҳолатини назорат этиш учун методик тавсиялар ишлаб чиқарилган. Банклар хавфсизлик хизмати

ва ҳуқуқни муҳофаза қилувчи ташкилотлар томонидан ахборот хавфсизлиги инцидентларини тергов қилиш вақтида қаллобчилик қилган шахслар жиноий жавобгарликга тортилмоқда.

Ахборот хавфсизлиги инцидентларини тергов қилиш хусусиятлари. Етказилган зарар минимал бўлишидан қатъий назар улар билан курашиш керак. Чунки кўп ҳолларда тергов давомида жуда катта хатоликлар аниқланади. Ҳужум излари аниқланади ва ҳимоя қандай ишлаши яна бир бор тестланади. Бунда ахборот хавфсизлиги инцидентларига одатда банкларни ахборот хавфсизлиги сиёсати қоидаларини бузиш киради. Улар орасидан рухсат этилмаган нусхалаш, интернетнинг ташқи адресларига маълумот юбориш ёки махфий маълумотларни чоп этиш, ўртанилган қоидаларни бузиш, ахборотга тасодифий таъсирлар, вируслар ва зараркунанда дастурлар билан зарарланиши ва ҳамда шахсий мақсадларга ахборот ресурсларидан фойдаланишлар киради. Бунда ахборот хавфсизлиги инцидентларининг пайдо бўлишига фойдаланувчилар билимсизлиги сабаб бўлади. Баъзи бир фойдаланувчилар ҳеч ким уларни устидан назорат қилмаётгани учун шундай хатоликлар содир этадилар.

Интизомий жавобгарлик. Тажрибада ахборот хавфсизлиги инцидентлари классификацияси эксперт усуллар орқали, лекин одатда қоида бўйича турли мутахассислар томонидан амалга оширилади. Худди мана шу жараёнда тизимлиликни ва инцидентни классификацияси ва келажакда жавоб қайтариш учун қарор қабул қилишда субъективизмни камайтириш даражасини ошириш зарур ҳисобланади. Бу эса ўз навбатида қоидаларни олдиндан тайёрлаб бориш, ўқитиш ва ҳар доим текширувда сақлаш билан амалга оширилади. Эксперт ечим топишни математик кўринишини қурилмавий аниқ бўлмаган мантиқ ёрдамида ифодалаш мумкин, бундай усул билан биз керакли натижани аниқ бўлмаган ҳолатларда ҳам топиш мумкин. Эксперт тажрибаси асосида ахборот хавфсизлиги инциденти классификациясини мантиқий-лингвистик модели қурилади. Бунда у кирувчи ва чиқувчи мантиқий лингвистик қийматлар билан ифодаланади ва улар ўзаро қандайдир эвристик қоидалар билан боғланади (9.1-жадвал).

9.1-жадвал

Ахборот хавфсизлиги инциденти классификациясини мантиқий-лингвистик модели

1.	“Агар<вазият 1> бўлса унда <ҳаракатни амалга ошир 1>”
2.	“Агар<вазият 2> бўлса унда <ҳаракатни амалга ошир 2>”.
....	……
N	“Агар<вазият n> бўлса унда <ҳаракатни амалга ошир n>”.

Ахборот хавфсизлиги инциденти классификацияси амалга оширилгандан сўнг инцидентга жавоб қайтариш ҳаракати бошланади. Бунинг учун банкда ахборот хавфсизлиги инциденти классификациясини аниқланган алгоритми маълум бўлиши зарур. Бундай аниқлик даража “ҳеч қандай натижасиз” ёки “аҳамиятсиз” гуруҳланса ҳам унга жавоб барибир бўлиши лозим.

Маълумотлар базасини шакллантириш. Ахборот хавфсизлиги инцидентларига жавоб қайтаришда мавжуд факторлар-бу ахборот хавфсизлиги инцидентлари базасига мос келувчи ҳужжатларни тўғри юритишдир. Бу ўз навбатида материалларни текшириш учун йиғиш ва бирлаштириш имконини беради. Огоҳлантирувчи чора-тадбирларни қўллашда ахборот хавфсизлиги инцидентларига жавоб қайтариш жараёнидаги асосий мақсад негатив оқибатларни камайтиришдир. Шу билан бирга инцидент ёпилгандан кейин кўриладиган чора тадбирлар қуйидагилардир (хафсизлик сиёсатини ўзгаритиш, яхши бўлмаган ресурсларни ёпиб қўйиш ва ҳ.к). Ходимлар билан профилактик ишларни амалга ошириш қуйидагиларни ўз ичига олиши мумкин:

- қоидабузарга жазоларни қўллаш;
- қоидабузарга негатив имидж яратиш;
- фойдаланувчиларни ўқитиш ва қўшимча маслаҳатлар бериш;
- ахборот хавфсизлиги талабларига риоя қилувчи қўлланмаларни тарқатиш;
- банк ахборот хавфсизлиги сиёсатига ўзгартиришлар киритиш ва ҳ.к.

Умумий ҳолда ахборот хавфсизлиги инцидентларини бошқариш жараёнини тезкорлиги ва самарадорлиги қуйидаги факторларга боғлиқ бўлади:

- жалб қилинган барча сатҳлар координациялаштирилган ҳолда ишлаши;
- инцидент билан боғлиқ ахборотни таҳлили ва олиш имкониятларини мавжудлиги;
- олинган натижаларни тўғрилиги ва тезкорлиги.

Ишни бажариш учун вазифа ва топшириқлар

1. Ахборот хавфсизлиги инцидентлари бошқариш тизимини тадбиқ этиш ва фойдаланиш.
2. Ахборот хавфсизлиги стандартлари.
3. Жавоб қайтариш алгоритми.
4. Маълумотлар базасини таърифи.
5. Дастурий модуль ишлаб чиқиш.

Фойдаланилган адабиётлар

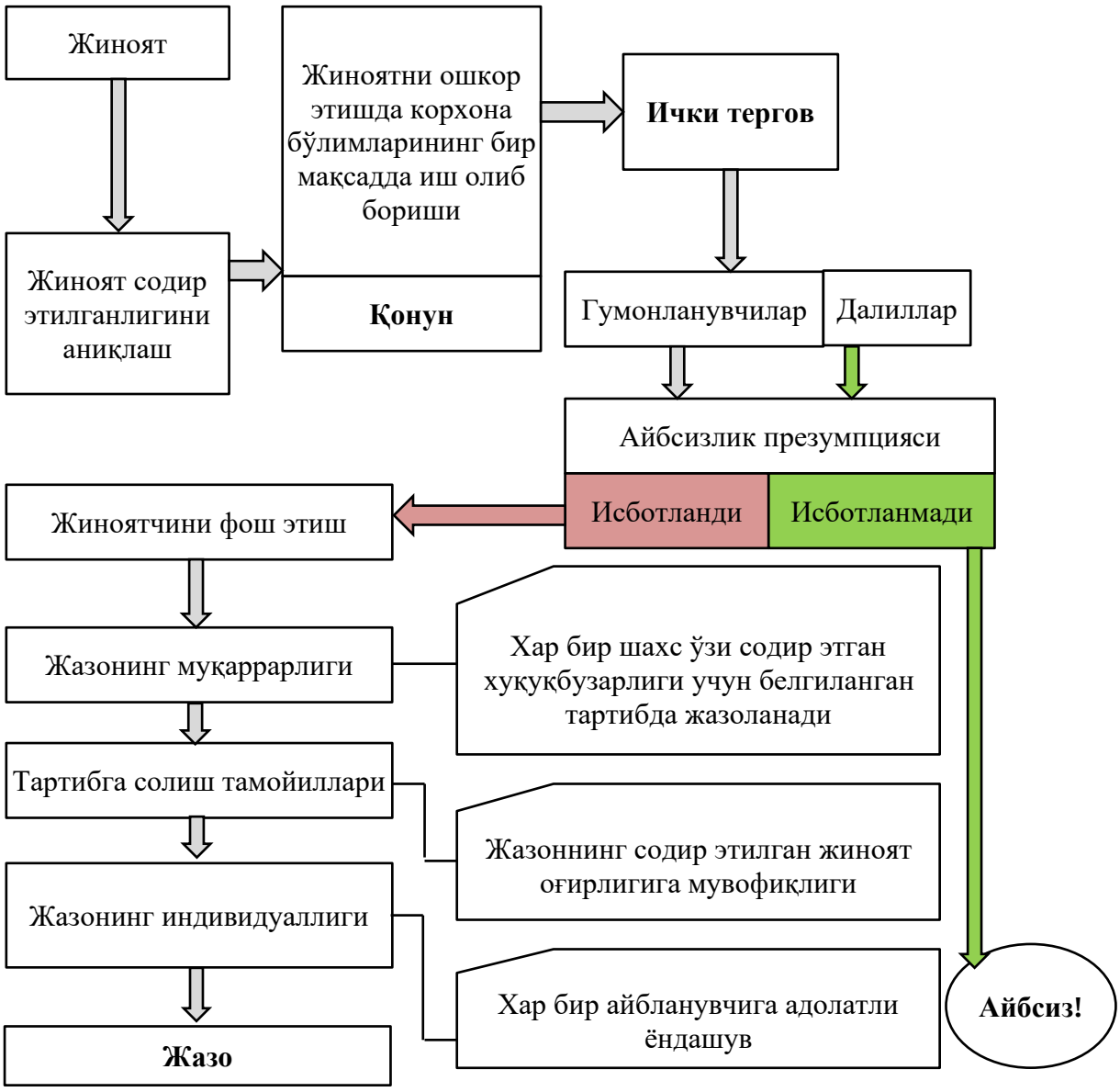
1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.

10-АМАЛИЙ МАШҒУЛОТ

Мавзу: Корхонада ахборот хавфсизлиги инцидентларини тергов қилиш ва уларни баҳолаш усуллари

Ишдан мақсад: Корхонада ахборот хавфсизлиги инцидентларини тергов қилиш ва уларни баҳолаш усулларини ўрганиш.

Назарий қисм: Ички терговнинг мақсади – содир бўлган инцидентга айбдорни топиш, юз берган инцидентнинг сабабини аниқлаш, келажакда бундай ходисаларга дуч келмаслик учун талаб ва таклифлар ишлаб чиқиш.



10.1-расм. Корхонада ахборот хавфсизлиги инцидентларини тергов қилишни ташкил этиш

Ички тергов ўтказишнинг асосий вазифалари: ишчининг нима сабабдан, қандай вазият ва шароитда жиноят содир этганлигини аниқлаш; жиноятга дахлдор аниқ бир шахс ёки шахсларнинг айбдорлик даражасини аниқлаш; жиноят содир этиш турларини, сабабини ва шароитини бартараф этиш учун

огоҳлантириш-профилактик турдаги тадбирлар ташкил этиш ва ўтказиш бўйича тавсиялар ишлаб чиқиш (10.1-расм).

Ишнинг бажарилиш тартиби. Ахборот хавфсизлиги инцидентларини тергов қилиш, аниқлаш, тахлил қилиш ва бахолаш. Инцидентларга қарши чора кўришда бу босқичларнинг ўз вақтида бажарилиши ва хаққонийлигига қараб, унинг муваффаққиятли ишлашини таъминлаб бериш.

Жазонинг муқаррарлиги тамойилини амалга ошириш - юридик жавобгарлик самарадорлиги ва унинг вазифаларини бажаришда мухим шартлардан бири хисобланади.

Маъсулият муқаррарлиги принципи, шаҳснинг расмий ёки материал ҳолатидан қатъи назар ўзи содир этган ҳуқуқбузарлиги учун белгиланган тартибда жазоланишини англатади.

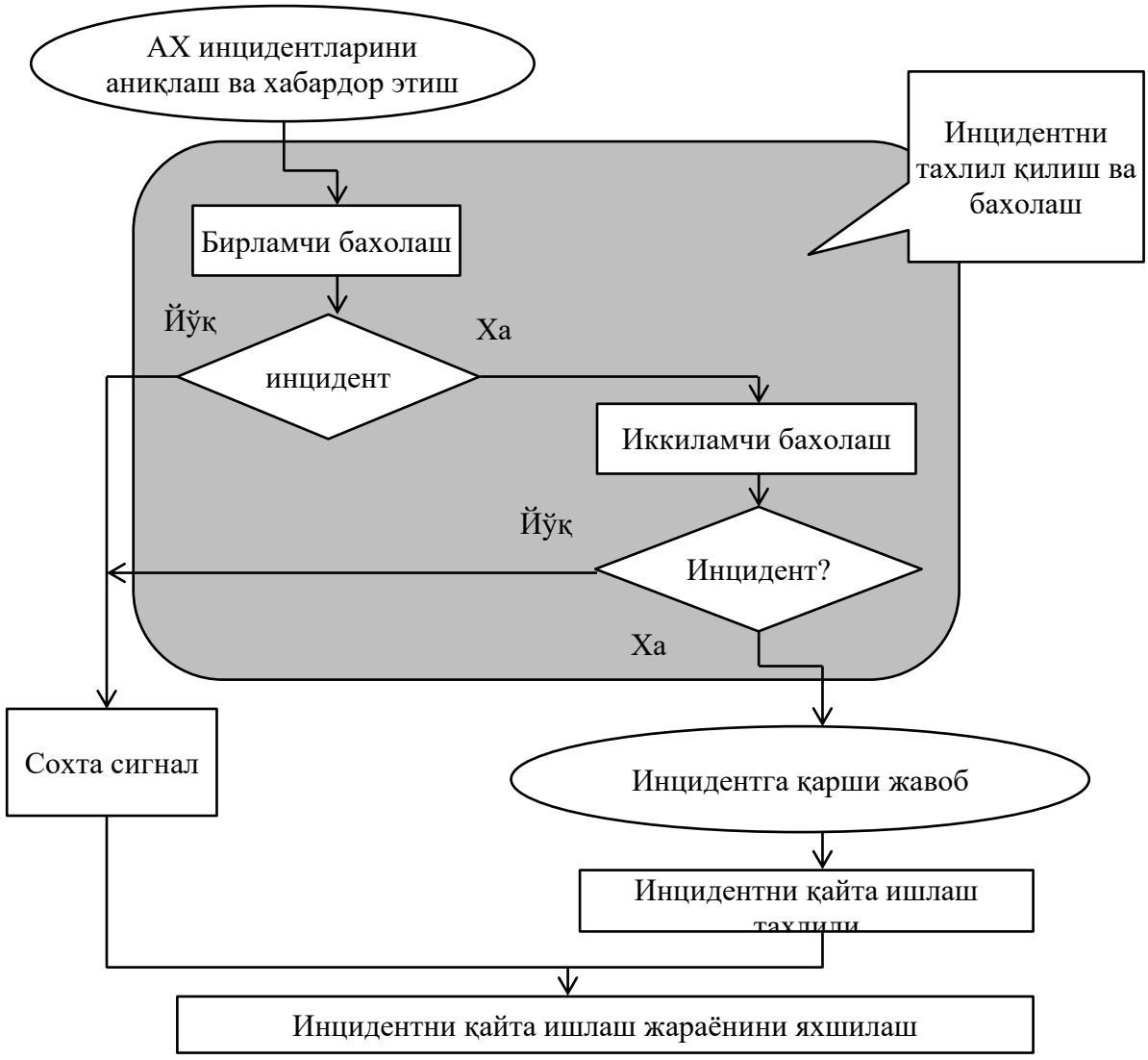
Жазонинг муқаррарлиги принципи маъсулият муқаррарлиги приниципи - айбсизлик тахминига зид бўлмаслиги керак. Жиноят содир этган ҳар бир айбланувчи унинг айбдорлиги қонунда кўрсатилган тартибда исботланмагунга ва қонуний кучга эга ҳукмда кўрсатилгунга қадар айбсиз ҳисобланади.

Ички терговни ташкил этиш. Асосий босқичлар. Корхонада ички тергов ўтказишни ташкил этиш, ички хавфсизлик бўлими зиммасига юклатилади. Ички тергов ўтказиш учун корхона раҳбари томонидан комиссия ташкил этилади. Айрим холларда тергов ахборот хавфсизлиги назорати маркази мутахассиси томонидан ўтказилиши мумкин. Комиссия аъзолари сафига жиноятнинг хусусиятига қараб, корхонанинг ходимлар бўлими ишчилари ва бошқа идоравий бўлимларидан ишчи ходимлар киритилади. Комиссия ишининг бажарилиш муддати, тўлиқлиги ва холислиги раис томонидан ташкиллаштирилади, ходимлар томонидан бажарилади. Тергов ўтказиш муддати одатда корхона раҳбари томонидан кўрсатилади. Ички тергов натижалари тергов якунланганидан сўнг хизмат ҳужжатлари орқали расмийлаштирилади. Тергов материаллари ички хавфсизлик бўлимида бир неча йил давомида сақланади, ундан кейин архивга топширилади.

Корхонада ахборот хавфсизлиги инцидентларини баҳолаш усуллари. Ахборот тизимлари сонининг ўсиши ва ахборот технологияларининг такомиллашгани сари, ахборот хавфсизлигидаги инцидентларнинг сони ҳам ортиб бормоқда.

Халқаро стандарт ISO 27001:2005 ахборот хавфсизлиги инцидентларини бошқариш тартибини яратиш зарурлигига алоҳида эътибор қаратади. Чунки, Ахборот хавфсизлигини самарали бошқариш учун инцидентларга ўз вақтида жавоб қайтариш, уларнинг сабаби ва келиб чиқадиган оқибатларнинг олдини олиш зарур.ISO/IEC 27035 халқаро стандарти ва ГОСТ Р ISO 18044:2007

миллий стандартда ахборот хавфсизлиги инцидентларини бошқариш жараёнлари келтирилган. хуқуқий-меъёрий хужжатлар, ресурслар, таъминлаш каби масалалар, хусусан АХ инцидентлари таснифланиши, АХ инцидентларини тартиблашда ролларни тақсимлаш кўриб чиқилади. Айрим холларда корхонада АХ инцидентларни аниқлаш методикаси йўқ, ишчилар хар доим хам ишдаги асосий вазифаларнинг узилишларига алоқадар бўлмаганлиги сабабли, қандай ходисалар ахборот хавфсизлиги инциденти эканлиги ҳақида билмайдилар.



10.2-расм. Ахборот хавфсизлиги инцидентларини қайта ишлашни бошқариш

Ахборот хавфсизлиги инцидентларини тахлил қилиш ва баҳолаш ҳам, содир бўлган инцидент ҳақида маълумотнинг, унинг келиб чиқиш сабаби ва оқибатининг тўлиқ эмаслиги қийин бўлиши мумкин. Ахборот хавфсизлиги инцидентлари ва инцидентларининг актуал базасини яратиш ва таъминлаш эхтиёжи мавжуд. Ахборот хавфсизлиги инцидентлари ва инцидентлари базаси ахборот хавфсизлиги инцидентларини тартибловчиларнинг шахсий тажрибасига асосланиб яратилиши мумкин. Одатда корхона, хусусан йирик

фирма, компанияларда содир этилган ахборот хавфсизлиги инцидентлар хақида маълумотлар, тизимга қайта хавфнинг олдини олиш мақсадида ва корхона обрўсига зарар етказмаслик мақсадида нашр этилмайди (10.2-расм).

Лекин ахборот хавфсизлиги аналитиклари ахборот хавфсизлигини таъминлашда корхона кўрсатмасидан ташқари, ушбу инцидентлар содир бўлган муаммоларни ўрганиш, масалан, ишлаб чиқариш ва бошқа ташкилотларда, ахборот технологияларида топилган заифликлар ва муайян бир муддатдаги ахборот хавфсизлиги инцидентлари статистикаси хақида қисқача маълумот тақдим этишади. Бундай турдаги маълумотлар ахборот хавфсизлиги инцидентлари базасини актуал ҳолатда сақлаб туриш учун базани доимий янгилаб туришда имкон яратади. Ахборот хавфсизлиги инцидентларини тахлил қилиш ва бахолаш ахборот хавфсизлиги ходисаларини инцидент сифатида идентификация қилиш учун зарур бўлган маълумот миқдорининг катталиги сабабли, ушбу ходисаларнинг сабаби ва манбаларини аниқлаш хамда салбий оқибатларининг тарқалишида қийинчилик туғдиради, шунинг учун ушбу жараёнлар расмийлаштирилган ва автоматлаштирилган бўлиши зарур.

Ахборот хавфсизлиги инцидентларини унинг омиллари асосида бахолаш. Дастлабки ахборот хавфсизлиги инцидентси идентификациясини ахборот хавфсизлиги инциденти сифатида баҳолаш, инцидентнинг муайян бир турига кўрсатувчи АХ ходисалари омиллари асосида амалга ошиши мумкин. Ахборот хавфсизлиги ходисаси омили бу – ахборот хавфсизлиги ишдан чиққанлигига ишора берувчи ахборот хавфсизлиги инцидентси аломати, ҳамда хавфсизлик билан боғлиқ кутилмаган инцидент рўй бериши. Инцидент омиллари ахборот хавфсизлиги инцидентлари тартиблаштирувчилар томонидан тизимни мониторинг қилиш жараёни ва режаланган текширувларда, ёки корхона ишчилари томонидан асосий иш вақтида техник воситалар орқали аниқланиши мумкин.

Тизимдаги салбий инцидентлар, масалан ишнинг секинлашуви, дастурий таъминотнинг ишдан чиқиши ва х.к. ҳар доим ҳам ахборот хавфсизлиги инциденти бўлмайди, шу сабабли ушбу инцидентлар омилининг фаол эканлигини тасдиқлаш мақсадида иккиламчи баҳолаш ўтказилади. Иккиламчи баҳолаш натижаларига қараб инцидентнинг рост ёки ёлғонлиги ҳақида қарор қабул қилинади. Ахборот хавфсизлиги инцидентини идентификация қилиш мақсадида мутахассисга манбадан аниқланган ахборот хавфсизлиги инцидентларининг маълумотлари асосида ахборот хавфсизлиги инцидентлари омилларига мос белгиланган рўйхатда берилади. Ахборот хавфсизлиги инцидент омиллари рўйхати содир бўлган инцидентлар маълумотлари базаси асосида тузилади ва доимий янгиланиб туради. Сўнгра

мутахассис батафсил кўриб чиқиш мақсадида инцидентнинг турини танлайди. Танланган инцидент турига мос равишда дастур орқали унга сценарий қурилади. Ишлаб чиқилган дастурий воситада аниқланган омилларга тегишли қўшимча маълумотлар ва фаоллигини тасдиқловчи инцидентларни йиғишга асосланган иккиламчи баҳолаш функцияси кўзда тутилган. Изоҳда хар бир инцидентга омилларни тасдиқловчи ёки инкор этувчи ва ушбу маълумотнинг манбасига қандай қўшимча маълумот кераклиги хақида маълумотлар келтирилган. Дастур иккиламчи баҳолашда тасдиқланган омилларга мос равишда инцидентнинг сценарийсини қайта қуриб чиқади. Бундан ташқари, дастурий восита омиллари белгиланмаган инцидентларнинг барча мумкин бўлган сценарийларини қуриш имконини беради. Бу функция инцидентларни қайта ишловчи мутахассисга кўриб чиқилаётган ахборот хавфсизлиги инциденти хақида қўшимча маълумотлар тўплаш ва унга қарши чора кўришда қарор қабул қилиш учун ҳаққонийлигини оширишга имкон беради. Дастурий восита потенциал инцидент содир бўлиш эҳтимолини алоҳида сценарийлари бўйича салбий инцидентлар нисбийлигига ва уларни олдини олиш бўйича химоя чораларига мувофиқ баҳолашга имкон беради. Бунинг учун дастурда 5 даражали химоя чоралари ўрнатилган, 0 дан (химоя чоралари мавжуд эмас) 4 гача (химоя чоралари инцидент сценарийларининг салбий ходисаларини олдини олади). Ҳар бир даражага $z-$ химоя чораларининг натижавий коэффициенти мос келади. Масалан, агар 0.25 га тенг даража оралиғидаги қадам танланса, у холда 1 даражали химоя чоралари учун натижавийлик коэффициенти 0.75 га тенг бўлади, (яъни ушбу химоя чораларини қўллаганда инцидент инцидентларининг содир бўлиш эхтимоллиги 0.25 га камаяди), 2 даражали ҳимоя чоралари учун натижавийлик коэффициенти 0.5 га тенг бўлади (яъни ушбу химоя чораларини қўллаганда инцидент ходисаларининг содир бўлиш эхтимоллиги 0.5 га камаяди) ва х.к. Инцидент сценарийларидаги салбий ходисаларнинг содир бўлиш эҳтимоллигини қуйидагича аниқлаш мумкин:

$$P_{HC} = h_1 z_i$$

Бу ерда

P_{HC} −инцидентларнинг содир бўлиш эхтимоллиги, $i = 1, n$;

n −инцидент сценарийсида салбий ходисаларнинг сони;

h_1 − инцидентнинг қайтарилиши;

z_i −инцидент сценарийсидаги салбий инцидентларни олдини олишга қаратилган химоя чораларининг натижавийлик коэффициенти.

Инцидентнинг алохида сценарий бўйича содир бўлиш эхтимоллиги P_N қуйидаги формула орқали ан

10.3-расм. Ахборот хавфсизлиги инцидентларини баҳолашнинг блоксхемаси

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

АХ инцидентининг зарарли дастурий таъминотга тадбиқ қилиш инциденти мисолида алоҳида сценарий бўйича содир бўлиш эҳтимоллигини аниқлаш натижаси (10.3-расм) да келтирилган.

Ахборот хавфсизлиги инцидентлари ва инцидентлари актуал маълумотлар базаси асосида, тизимда содир бўлаётган ахборот хавфсизлиги инцидентларини баҳолаш имконини беради.

Шу орқали вақтни тежашда ва аниқланган ахборот хавфсизлиги инцидентларини қайта ишлашда етарли қарор қабул қилиш учун маълумотларнинг хаққонийлигини оширишга хисса қўшади.

Ишни бажариш учун вазифа ва топшириқлар

1. Ахборот хафсизлиги инцидентларига жавоб қайтариш алгоритмини вазифаси.
2. Ички терговнинг мақсади?
3. Корхонада ахборот хавфсизлиги инцидентларини тергов этишни кетма-кетлиги.
4. Ахборот хавфсизлиги инцидентларини унинг омиллари асосида бахолаш дастурини ишлаб чиқиш.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.
3. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».
4. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». – М.: Стандартинформ, 2009. – 50 с.

11-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги сохасида жиноятларнинг криминал таснифи

Ишдан мақсад: Ахборот хавфсизлиги соҳасида жиноятларнинг криминал таснифи таҳлил этиш.

Назарий қисм: Хорижий мамлакатлар томонидан компьютер жиноятларини содир этиш бўйича турлича таснифлар ишлаб чиқилган. Қуйида шу каби содир этиладиган жиноят турларининг номланиши Интерпол бош котибияти кодификаторига мувофиқ келтирилган. 1991 йилда ушбу кодификатор қидирув автоматлаштирилган тизимига бириктирилган.

Компьютер жиноятларини ифодаловчи барча кодлар Q харфи билан бошланувчи идентификаторларга эга. Жиноятнинг тавсифланиши учун камайиб бориш тартибида жойлашган бештагача код ишлатилиши мумкин. (11.1-жадвал).

11.1-жадвал

Компьютер жиноятларни тавсифловчи кодлар

QA	Рухсатсиз кириш ва тутиб олиш
QD	Компьютер маълумотларини ўзгартириш
QF	Компьютер фирибгарлиги
QR	Ноқонуний нусҳа олиш
QS	Компьютер саботажи
QZ	Бошқа компьютер жиноятлари

QA – **Рухсатсиз кириш ва тутиб олиш**

QAH - компьютерни қўлга олиш

QAI – тутиб олиш

QAT – вақтни ўғирлаш

QAZ – Рухсатсиз кириш ва тутиб олишнинг бошқа турлари

QD – **Компьютер маълумотларини ўзгартириш QUL** – мантиқий бомба

QDT – троя оти

QDV - компьютер вируси

QDW - компьютер чувалчанги

QDZ – бошқа маълумотларни ўзгартириш турлари

QF - Компьютер фирибгарлиги

QFC – банкоматларда фирибгарлик

QFF - компьютер орқали қалбакилаштириш

QFG – ўйин автоматларида фирибгарлик

QFM – киритиш ва чиқариш дастурларида манипуляция қилиш

QFP – тўлов воситаларида фирибгарлик

QFT – телефон фирибгарликлари
QFZ – бошқа компьютер фирибгарликлари
QR – Ноқонуний нусха кўчириш
QRG – компьютер ўйинлари
QRS – бошқа дастурий таъминотлар
QRT – яримўтказгич махсулотлар топографияси
QRZ – бошқа ноқонуний нусҳа кўчириш
QS - Компьютер саботажи
QSH - аппарат таъминот билан
QSS – дастурий таъминот билан
QSZ – саботажнинг бошқа турлари
QZ – Бошқа компьютер жиноятлари
QZB - компьютер эълонлар тахтаси ёрдамида
QZE – тижорат сири хисобланган маълумотни ўғирлаш
QZS – махфий бўлган маълумотни узатиш
QZZ – бошқа компьютер жиноятлари

Келтирилган кодификаторга мувофиқ бир нечта компьютер жинояти турларининг қисқача тавсифи:

Рухсатсиз кириш ва тутиб олиш *(QA) қуйидаги компьютер жиноятларини ўз ичига олади.*

QAH – «Компьютерни қўлга олиш» (хакинг - hacking): Кириш хуқуқига эга бўлмаган холда компьютер ёки тармоққа кириш. Ушбу компьютер жинояти тури одатда хакерлар томонидан ўзга ахборот тармоғига киришда қўлланилади.

QAI – тутиб олиш (interception): Кириш хуқуқига эга бўлмаган холда техник воситалар ёрдамида маълумотни қўлга олиш. Бу жараён тўғридан тўғри тизимнинг ташқи коммуникацион канали, ёки қўшимча қурилмаларга бевосита боғланиш орқали амалга оширилиши мумкин. Бунда кабел-сим тизимлари, ер усти микротўлқинли тизимлари, суньий йўлдош алоқа хамда тизими хамда махсус хукумат алоқа тизими, кузатилаётган обьект хисобланади. Бундай турдаги компьютер жиноятларига шунингдек электромагнит қўлга киритиш хам киради (electromagnetic pickup). Замонавий техникалар компьютер тизимига боғланмасдан маълумотларни қўлга киритишга имкон беради. Қўлга киритиш марказий процесор, монитор, коммуникацион кабел, принтер ва х.к. нурланиши туфайли амалга ошади. Бунинг хаммасини обьектдан етарли масофада туриб ҳам амалга ошириш мумкин.

Тасдиқланмаган кириш ва қўлга олиш усулларини таснифлашда қуйдаги махсус терминлар қўлланилади:

*«Жучок»(*bugging) - "қўнғизча" деганда, хизмат кўрсатилаётган таркибнинг сухбатини қўлга киритиш мақсадида компьютерга микрофон ўрнатиш тушунилади;

*«Откачивание данных» (*data leakage) – "маълумотларни суғуриб олиш" тизимга таалуқли асосий маълумотни қўлга киритиш мақсадида керакли маълумотлар тўплаш;

«Уборка мусора» (scavening) – "ахлатни тозалаш" фойдаланувчи компьютерда ишни якунлаганидан сўнг маълумотларни қидириш. Бу усул икки турга бўлинади – жисмоний ва электрон. Жисмоний турида ахлат қутиларини кўздан кечириш ва х.к. назарда тутилади.

QAT – вақтни ўғирлаш: пул тўламаслик мақсадида компьютер тизими ва тармоғидан ноқонуний фойдаланиш.

Компьютер маълумотларини ўзгартириш (QD) ўз ичига қуйидаги жиноятларни олади:

QDL/QDT - мантиқий бомба (logic bomb), троя оти (trojan horse): мантиқий бомба ва троя отини жорий этиш йўли билан ноқонуний компьютер маълумотларини ўзгартириш.

Мантиқий бомба дастурга командалар тўпламини махфий ўрнатади, натижада муайян муддатда фақатгина бир марта ишга тушади.

Троя отининг мақсади тизимнинг иш фаолияти сақланиб қолган ҳолда дастурга фойдаланувчи режалаштирмаган ўзга функцияларни бажариш командаларини киритишдан иборат.

QDV - вирус (virus): компьютер вирусини тарқатиш орқали ноқонуний компьютер маълумотлари ёки дастурларини ўзгартириш.

Компьютер вируси – бу компьютерда салбий оқибатларга олиб келувчи, ўзини бошқа дастурга ёзиш, кўпайиш ва янги вируслар яратиш имконига эга махсус ёзилган дастур.

Вирус дастури билан компьютерни юқтириш ва уни даволаш тиббий амалиёт каби бир қанча хусусиятга эга. Умуман олганда бу термин тиббиётга жуда яқин:

- резервлаш – FAT нусха кўчириш, файлларнинг ўзгариши хақида кунлик архив тўлдириш - бу вируслардан ҳимояланишнинг энг мухим ва асосий усули хисобланади. Бошқа усуллар умумий химоя даражасини юқори таъминласада, кунлик архивлашни ўрнини эгаллай олмайди;
- профилактика – янги сотиб олинган ва эксплуатация қилинган дастурларни алоҳида сақлаш, дискларни алохида "сув ўтмайдиган бўлинма", "фақат ўқиш учун" режими ўрнатилган қисмларда сақлаш, ишлатилмаган дастурларни архивларда сақлаш, дискетлардан янги дастурларни ёзиш учун махсус "инкубацион" қисмдан фойдаланиш, ишлатилаётган дискетларнинг

BOOT-секторини тизимли текшириш ва х.к.;

- таҳлил – янги олинган дастурларни махсус воситалар орқали текшириш ва назоратдаги мухитда ишга тушириш, дастурни сақлашда ва узатишда контроль суммани тизимли қўллаш. Хар бир контроль суммасиз олинган янги дастур ваколатли мутаҳассислар томонидан камида компьютер вирусларининг маълум турларига текширилиши ва маълум бир вақт ичида унинг устидан назорат олиб борилиши;
- фильтрлаш – FluShot Plus, MaceVaccinee каби резидент дастурлардан ва бошқа ноқонуний харакатларни амалга оширишга уринишларни аниқловчи дастурлардан фойдаланиш;
- вакциналаштириш – файллар, дисклар, каталогларни махсус қайта ишлаш, дастур ёки дискнинг шикастланганлиги ушбу вирус тури билан мос келадиган махсус резидент-вакцина дастурларини ишга туширади;
- терапия (даволаш) – махсус антивирус дастурлар орқали дастурларда аниқланган вирусларни деактивация қилиш ёки дастур-фаг ёрдамида шикастланган файллар ва дискларни барча вирус нусхаларини йўқ қилиш йўли билан дастурнинг дастлабки холатини тиклаш.

Шуни айтиш мумкинки, компьютер вирусидан халос бўлиш профилактика ўтказишни таъминлашдан кўра анча қийин.

QDW - чувалчанг: чувалчангни компьютер тармоғига юбориш, жорий этиш ёки тарқатиш, компьютер маълумотлари ва дастурларини ноқонуний ўзгартириш.

Компьютер фирибгарлиги (QF) ўзининг таркибига турли хил жиноят содир эиш усулларини жамлаган:

QFC - банкоматлардан нақд пул ўғирлаш билан боғлиқ компьютер фирибгарлиги

QFF - компьютер сохталиклари: сохта қурилмалар (карточка) яратиш орқали компьютер тизимларида фирибгарлик ва ўғирлик

QFG - ўйин автоматлари билан боғлиқ фирибгарлик ва ўғирлик

QFM – киритиш-чиқариш дастурлари билан манипуляция қилиш: компьютер тизимларига нотўғри киритиш ва чиқариш орқали фирибгарлик ва ўғирлик қилиш ёки шу орқали дастурни манипуляция қилиш. Бу турдаги компьютер жинояти турларига маълумотларни киритиш-чиқариш жараёнида амалга ошувчи маълумотларни алмаштириш усули (data diddling code change), киритиш мумкин. Бу энг оддий ва шунинг учун энг кўп қўлланиладиган усул ҳисобланади.

QFP - Тўлов воситалари билан боғлиқ компьютер фирибгарлиги ва ўғирлиги. Ушбу тур компьютер орқали пул воситаларини ўғирлаш бўйича. Компьютердан фойдаланишдаги жиноятларнинг 45 % ни аксарияти ушбу тур,

яъни пул воситаларини ўғирлаш билан боғлиқ жиноятлар ташкил этади.

QFT - телефон фирибгарлиги: телефон тизимига хизмат кўрсатувчи телекоммуникацион хизматларга компьютернинг протоколлари ва процедураларига тажовуз қилиш орқали кириш

Маълумотдан ноқонуний нусҳа олиш (QR) ўз ичига қуйидаги жиноятларни олади:

QRG/QRS – компьютер ўйинларини ва қонун ҳимоясидаги бошқа дастурий таъминотдан ноқонуний нусҳа олиш, тарқатиш ёки чоп этиш.

QRT – яримўтказгичли қурилмаларнинг топографиясидан ноқонуний нусҳа олиш: қонун ҳимоясидаги яримўтказгичли қурилмалар топографиясидан ноқонуний нусҳа олиш, яримўтказгичли қурилма ёки унинг топографиясини ноқонуний тижорат қилиш ёки шу мақсадда импорт қилиш.

Компьютер саботажи (QS) ўз ичига қуйидаги жиноятларни олади:

QSH – аппарат таъминот ёрдамида саботаж: киритиш, ўзгартириш, ўчириш, компьютер аълумотлари ёки дастурларини бостириш; компьютер ёки телекоммуникация тизимининг фаолиятига халал бериш мақсадида компьютер тизимига аралашиш.

QSS – дастурий таъминотли компьютер саботажи: компьютер маълумотларини ёки дастурларни ноқонуний ўчириш, зарар етказиш, яроқсиз ҳолатга келтириш.

Бошқа турдаги компьютер жиноятлари (QZ) қуйидагича таснифланади:

QZB - электрон эълонлар тахтаси ёрдамида (BBS) жиноий фаолиятга таалуқли маълумотларни сақлаш, алмашиш ва тарқатиш;

QZE – тижорат сири ҳисобланган маълумотни ўғирлаш: молиявий зарар етказиш ёки молиявий манфаат олиш мақсадида ноқонуний тижорат сирини қўлга киритиш ёки узатиш.

QZS - Махфий турдаги маълумотларни сақлаш, алмашиш ва тарқатиш ёки жойини алмаштириш учун компьютер тизимлари ва тармоқларидан фойдаланиш.

Баъзи бир компьютер жинояти бўйича мутахассислар қуйида келтирилган ноананвий номли манипуляция усулларини алохида гурухда келтиришади.

«Вақтинчалик бомба» - аниқ бир вақтда ишга тушувчи мантиқий бомбанинг бир тури;

«Асинхрон хужум» (asynchronous attack) компьютер тизими томонидан икки ва ундан ортиқ фойдаланувчилари командаларининг бажарилиши ва аралашуви натижасида хосил бўлади

«Моделлаштириш» (simulation modelling) жиноятчи аралашиши мумкин

бўлган жараёнларни таҳлил қилиш билан бир қаторда жиноят содир этишни режалаштириш учун хам қўлланилади. Натижада жиноят содир этиш усули "такомиллашуви" амалга ошади.

Ишни бажариш учун вазифа ва топшириқлар

1. Ахборот хавфсизлиги сохасида жиноятларнинг криминал таснифи тушунчаси.
2. Компьютер жиноятларни тавсифловчи кодлар.
3. Компьютер саботажи (QS) ўз ичига қандай жиноятларни олади?
4. Компьютер маълумотларини ўзгартириш қандай жиноят ҳисобланади?

Фойдаланилган адабиётлар

1. Ўзбекистон Республикаси президентининг Ўзбекистон Рекспубликаси Қонунчилик Палатасидаги 2013 йил 27 июндаги № ПФ-1989сонли "Ўзбекистон Республикасининг миллий ахборот-коммуникация тизимини янада ривожлантириш чора-тадбирлари тўғрисида" фармони, № 40, 528.б.
2. Савельева М.В., Смушкин А.Б. Криминалистика. Ўқув қўлланма. М,: «Дашков и К» шашриёт уйи нашри. - 2009 й. - 608 ISBN: 978-5-91131-836-9.
3. Федотов Н.Н. Форензика - Компьютерная криминалистика. - М.: Юридический мир, 2007.
4. Копырюлин А. Квалификация преступлений в сфере компьютерной информации // Законность. - 2007. - № 6. - С. 40-41.
5. Осипенко А. Уголовная ответственность за неправомерный доступ к конфиденциальной компьютерной информации // Уголовное право. - 2007. - № 3. - С. 43.
6. CMU/SEI-2004-TR-015 «Defining incident management processes for CISRT».

12-АМАЛИЙ МАШҒУЛОТ

Мавзу: Ахборот хавфсизлиги инцидентларини прецедентли таҳлил қилиш асосида тадқиқ этиш

Ишдан мақсад: Ахборот хавфсизлиги инцидентларини прецедентли тахлил ва тадқиқ этишни ўрганиш.

Назарий қисм: Умумий холда инцидентларни бошқариш циклик жараён бўлиб унинг асосий босқичларини PDCA модели акс эттиради. ISO 27001 стандартига асосан анъанавий модел бошқаришни тўртта босқичидан иборат:

- ахборот хавфсизлиги инцидентларини идентификатлаштириш;
- ахборот хавфсизлиги инцидентларига акс таъсир кўрсатиш;
- терговни амалга ошириш;
- коррекцияловчи ва олдини олиш тадбирлари

Инцидентга акс таъсир кўрсатиш ва терговни амалга ошириш пайтида ахборот тизимини конкрет заифликлари аниқлаштирилади, рухсатсиз кириш ва ҳужум излари намоён бўлади, химоя воситаларининг имконияти текширилади, тизим архитектурасини (бузилиши) ахборот хавфсизлиги сифати ва уни бошқариш мумкинлиги аниқланади. Шунингдек тахлил қилиш процедурасининг мавжудлиги ва инцидент оқибатларини олдини олиш ва қайтарилиш эхтимоллиги камайтириш чоралари кўрилишидир. Биринчи навбатда содир бўлиши мумкин бўлган инцидентни ўз вақтида аниқлаш лозим. Акс холда қисқа муддатда акс таъсир кўрсатиш мумкин бўлмай қолади. Шунингдек аниқланган инцидентларга нисбатан акс таъсир кўрсатиш чоралари ишлаб чиқилмаган. Бундай вазиятларни ҳал қилиш учун кўп вақт талаб этилади.

Ахборот хавфсизлиги инцидентларига акс таъсир кўрсатиш муаммолари. Инцидентларни бошқаришнинг асосий воситаларига мониторинг тизими ва ходисаларининг ахборот хавфсизлиги корреляцияси хисобланади, таҳлил натижалари асосида акс таъсир стратегияси ишлаб чиқилади. Мониторинг тизими шакллантирадиган ахборотдан катта хажми, юқори малакали Мутахассислардан иборат ахборот хавфсизлиги инцидентларига акс таъсир этувчи гуруҳнинг мавжудлигини талаб етади. Молиявий имкониятларнинг йўқлиги ва мутахассисларсиз инцидентларни бошқариш жараёни самарадорли ташкил етилишини хар доим хам имконияти бўлмайди. Қарор қабул қилиш ,босқичида экспертга фикрига тайаниб қолиш оперативликни камайтиради ва натижада талофатни кўпайтиради. Шундай қилиб, юзага келиши мумкин бўлган инцидентларга оператив акс таъсир кўрсатишдек долзарб муаммо мавжуд. Бир қатор аниқланган стратегиялардан бирини қўллаш масаласини ечиш, ёки мос келадиган стратегия йўқлигини

эътироф этиб уни ишлаб чиқиш. Хақиқатга явинлик услуби инцидентларга акс таъсир этиш муаммоси ечимини топишда бошқариш жараёнини автоматлаштириш воситалари сифатида прецедент (CBR) асосидаги тизимларни тақазо этади. Натижада инцидентларга акс таъсир этишни аниқлаш фаолиятини автоматлаштиради, самарадорлигини оширади, акс таъсирни амалга оширишини тезлаштиради ва ахборот хавфсизлигини бошқариш жараёнига интеллектуал ёндашиш имконини беради.

Прецедентли тахлил. Прецедентли тизимларда ечимни қидириш аналог тушунчасига таянади (хусусийдан хусусийгача қидириш). Прецедент ва жорий вазият обьект сифатида тасвирланади, улар учун аналогни топиш зарур ва прецедентлар учун зарур ва прецедентлар учун адолатли фактларни кўчириш эвазига, кўринаётган инцидент учун қисман хулоса қилиш.

Одатда прецедент ташкил топади:

- муаммоли вазиятнинг изохидан;
- муаммони бартараф этиш учун кўрилаётган ҳаракатлардан тўпланади;
- ва бази холларда- натижа (ёки прогноз) ни ечимини қўллаш.

Прецедентнинг муқобил тузилмасини кўп ўлчамли параметрик вектор кўринишида кўрсатиш мумкин.

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

Бунда $x_1, x_2, \dots x_p$ – вазият параметрлари, ушбу прецедентни изохи.

R –масаланинг бир ёки бир неча ечимлар тўплами (диагноз, тавсиялар). Прецедентлар асосида мулохаза тўртта асосий босқични ташкил этувчи CBR –цикл (прецедентлар асосида мулохаза цикли), бўлиб қуйидагилардан иборат:

- юзага келган вазият учун прецедентлар базасидан мос прецедентларни ажратиш;
- жорий муаммони ечимини топиш учун прецедентдан қайтадан фойдаланиш;
- ечимни қайта кўриш ва жорий муаммога мос равишда мослаштириш;
- қабул қилинган ечимни янги прецедент қисми сифатида сақлаш.

Конкрет предмет соха спецификациясини ва ечиладиган масалани хисобга олган холда соддалаштирилган CBR –цикл қўлланиши мумкин.

Шундай қилиб, прецедентлар аппаратини қўллашдан мақсад операторга тайёр ечимни чиқариб беришдан иборат. Прецедентларни ажратиш мослик функсиясини аниқлашга асосланган, унинг қиймати жорий вазиятни ва прецедентни ўхшашлигини аниқлайди. Белгилар фазосида мақсадни функсияга мос нуқта аниқланади ва ўлчов доирасида энг яқин прецедент олинади.

Формал нуқтаи назардан прецедент ўхшашлиги $g = (x_{g1}, x_{g2}, \dots x_{gp})$ ва

жорий вазият $k = (x_{k1}, x_{k2}, \dots x_{kp})$ қуйидаги функция кўринишида ифодаланади.

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

Бунда $sim(x_{gi}, x_{ki})$ прецедентдан i- белгисини қийматини ва k жорий ходисадан (инцидент) i-белгиси локал ўхшашлиги. F функция прецедентдан жорий вазият билан тўлиқ мослигини ифодалайди. Базада ўхшаш прецедентлар йўқ бўлганда, ушбу усул юзага келган вазият учун ечимни топмайди. Ушбу муаммони ҳал қилиш учун CBR –циклда базани хулоса қилиш жараёнида тўлдириш имконияти назарда тутилганда ечими топилади.

Прецедентли тахлилни қўллаш концепцияси.

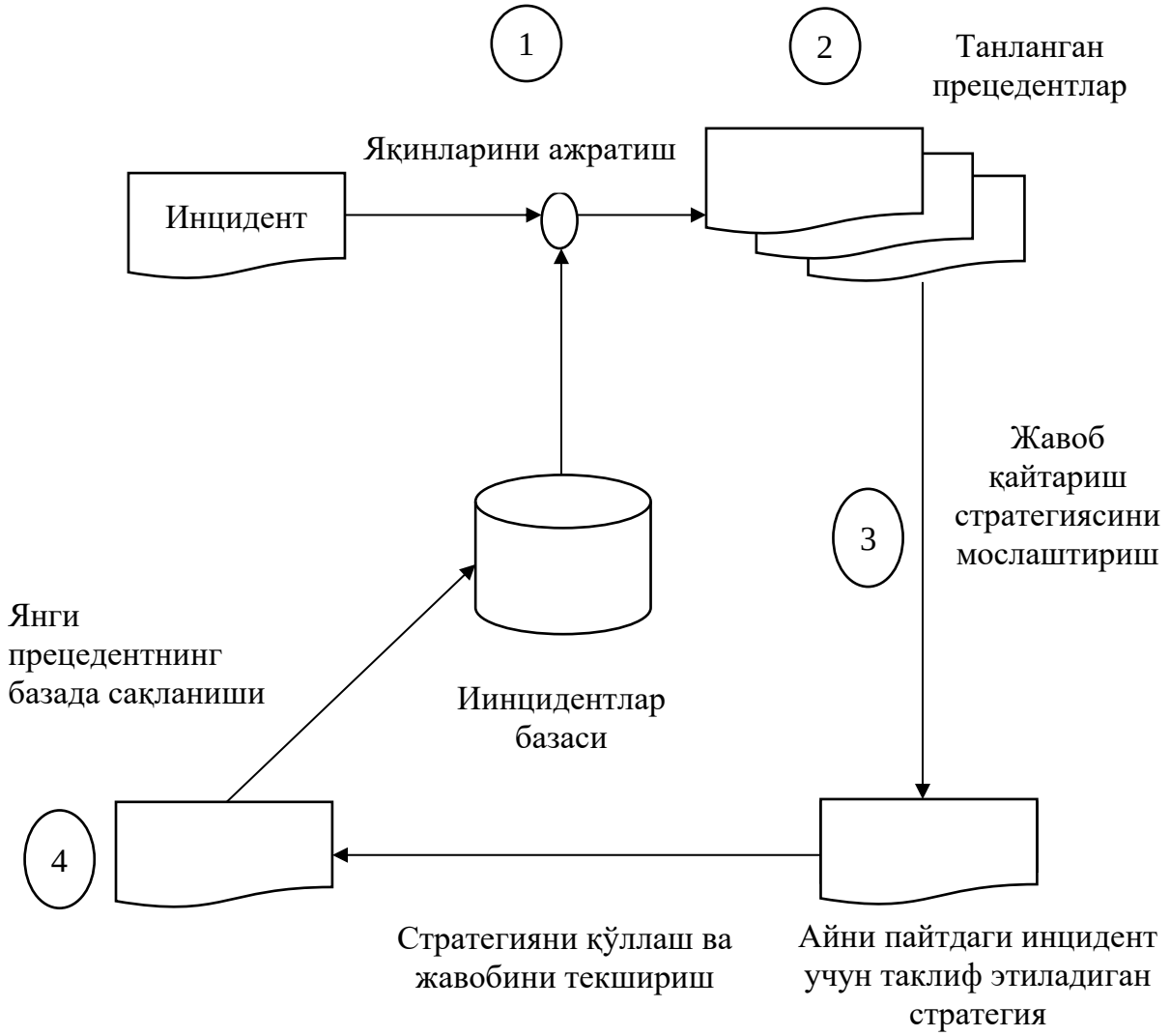
Юқорида айтиб ўтилганидек ахборот хавфсизлиги инцидентларини бошқаришнинг биринчи қадами инцидентларни рўйхатга олишдир. Кейинги ҳаракатлар ҳар битта инцидент учун классни хисобга олган холда акс таъсирни қўллашни таҳлил қилади. Ушбу босқичда қуйидаги муаммоларни ажратиш мумкин.

1. Ҳар доим ҳам инцидентларни классификациялаш тўғри бажарилмайди.
2. Ҳар битта инцидент ўзгача белгтларга ега бўлганлиги учун маълум тоифали инцидентларга акс таъсирдан ягона стратегия мавжуд эмас.
3. Олдин содир бўлмаган инцидентлар юзага келиши мумкин шунинг учун бундай инцидентлар учун мос равишда акс таъсир стратегияси мавжуд эмас.

Инцидентларни бошқариш жараёнини такомиллаштириш учун инцидентни таҳлил концепциясини қўллаш қуйидагилардан иборат. Маълум бўлган G - инцидентлар тўплами аниқланган R акс таъсир стратегиялари тўплами мавжуд. $G \to R$ га аксланиши прецедент яъни инцидентнинг изоҳи ва унга мос равишда таъсир стратегияси туридаги жуфтлик. Яъни инцидентни рўйхатга олганда унга мос равишда прецедент топилади. Шундан сўнг прецедент ечими ушбу инцидент учун қўлланади. Ушбу услубни амалга оширувчи тизимнинг мантиқий тузилиши 12.1-расмда келтирилган.

Олдин маълум бўлмаган инцидентлар ва улар учун акс таъсир стратегияси йўқ бўлган инцидентларни аномал инцидентлар деб атаймиз. Бошқача қилиб айтганда аномал инцидент деганда ҳимоя воситаси белгиланган инцидентга класс доирасида ўхшаши бўлмаган инцидентга айтилади.

Инцидентни аномаллиги тўғрисидаги хулоса ҳар томонлама таҳлил қилиш учун асос бўлади. Шуларни ҳисобга олган ҳолда прецедентли таҳлил инцидентларни нормал ва нормал бўлмаган синфларга ажратишни назарда тутади.



12.1-расм. Прецедентли таҳлил тизимининг мантиқий тузилиши

$G = \{g_1, \dots, g_n\}$ – прецедентлар тўплами;

$g_i = (x_1, \dots, x_p, r_i)$ – ягона прецедент;

$K = \{k_1, \dots, k_m\}$ – рўйхатга олинган инцидентлар тўплами;

$k_j = \{x_1, \dots, x_p\}$ – битта инцидент;

$F(g_i, k_j)$ – ўхшашлик функцияси;

$G_1 = \{g_i : F(g_i, k_j) \le d_{lim}\}$ – ўхшаш прецедентлар тўплами.

Шундай қилиб инцидентни прецедентлар тўпламига ўтказиш шарти қуйидагича ифодаланади:

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

Ифодадан кўриниб турибдики синфларга бўлиш натижаси чегаравий масофадан d_{lim} ва ўхшашликларнинг a_{lim}нинг энг кўп қийматига тўғридан тўғри боғлиқ.

Прецедентли таҳлил алгоритмининг модели. Тавсия этилган усулнинг самарадорлигини тадқиқ этиш учун KddDataset’99 маълумотлар

манбаидан фойдаланилади. Метрик синфлаш сифатида к –яқин қўшнилар методи қўлланилди. Ушбу босқичда охирги натижага ҳар бир параметрнинг таъсири маълум бўлмаганлиги учун, ўлчов бирликни оғирлик коэффицентларисиз олиш мақсадга мувофиқ. Матнли сценарийнинг алгоритми DeductorStudioAcademic таҳлил платформасидан ташкил топган (12.2-расм).

12.2-расм. Матнли сценарийнинг алгоритми

Рўйхатга олингандан сўнг нормалицация ўтказилади.

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

1. Алгоритм параметрларини инициализацияси: метрикани танлаш, d_{lim} масофа чегарасини ва a_{lim}га аналог чегара қийматини аниқлаш.

d_{lim} ни бошланғич қиймати сифатида синф масофаси киритилган:

Бу ерда, битта прецедентдан синфгача ўртача масофа

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

2. Метрика бўйича обьектлар орасидаги оралиқни ҳисоблаш

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

3. $d_{gk} \leq d_{lim}$ ифодани қаноатлантирувчи икки объектни аниқлаш. (прецедент g ва k инцидент ўхшаш ҳисобланади.

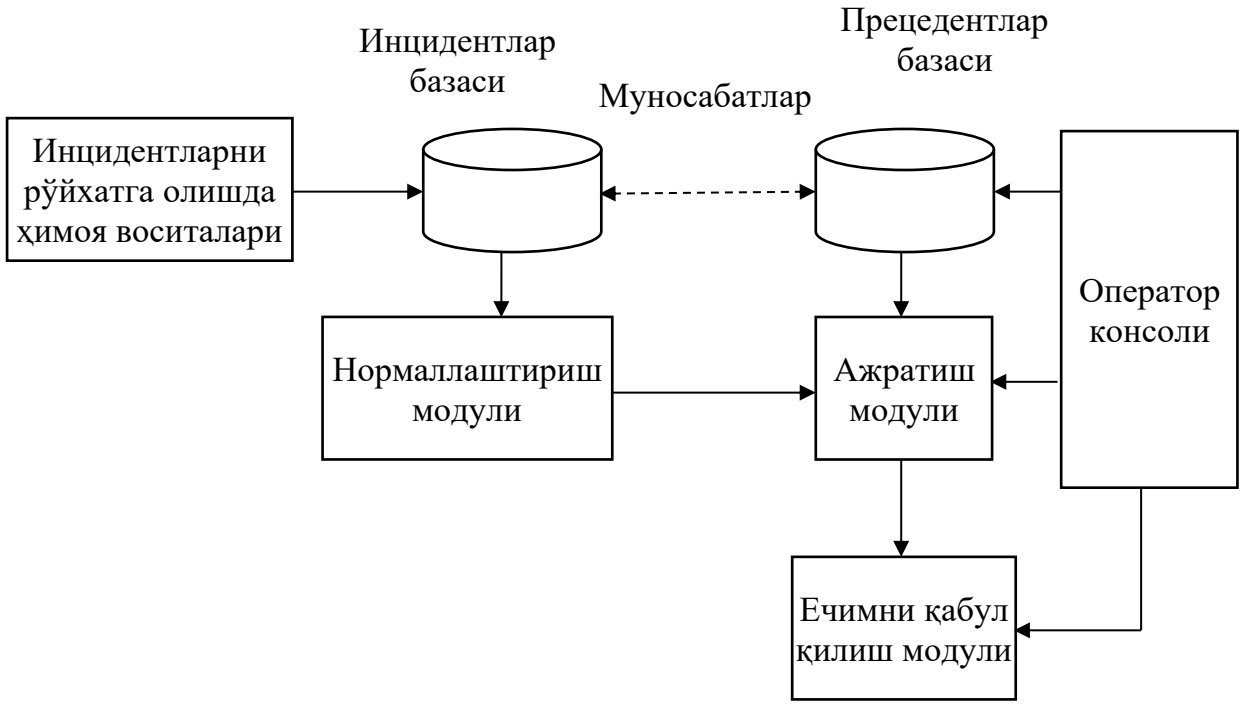
4. $d_{gk} \leq d_{lim}$. шартни бажарувчи ҳар бир k_j Инцидентга а прецедентлар сони ҳисобланади.

5. Инцидент k_j $a \leq a_{lim}$. бўлганда аномал деб кўрилади.

6. Таснифлаш натижасидан келиб чиқиб кейинги чоралар кўрилади.

7. Инцидентларни батафсил таҳлили ёки акс таъсир стратегиясини қўллаш.

Прецедентли тахлил тизими архитектураси. Прецедентли таҳлил тизимини дастурий ишлаб чиқилишига кўра, модулли тузилишга ега бўлиб қуйидаги компонентлардан ташкил топган.(12.3-расм).



12.3-расм. Прецедентли таҳлил тизими архитектураси

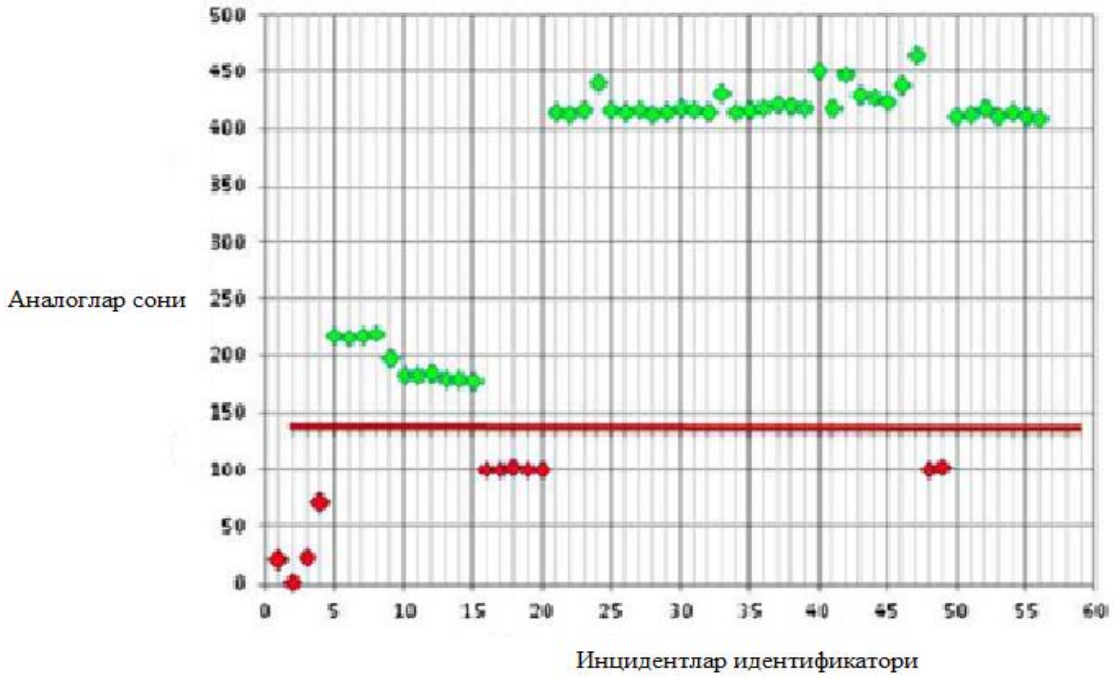
- рўйхатга олинган қайта ишлаш учун тайёрланган инцедентлар бўйича ёзувлар, инцидентлар базаси;
- маълумотларни нормаллаштириш модули, рўйҳатга олинган инцидентларни, прецедентларни базаси тузилишига кўра ўзгартирувчи;
- ажратиш модули, инцидент ва прецедентларни ўхшашлик катталикларини ҳисоблаш функцияси;
- қарор қабул қилиш модули, синфлаш натижасини аниқловчи ва инцидентни битта ёки бир нечта прецедентга катталиклар мослиги бўйича

ўхшашликни ўрнатиш;

- оператор консоли, аввал ноъмалум бўлган шартлар учун ишлаб чиқилган стратегияни мослаштириш ва таҳлил жараёнини коррециялаш учун мўлжалланган.

Шундай қилиб, прецедентли анализ концепциясини восита сифатида қўллаш, ахборот хавфсизлиги инцидентларини бошқариш жараёнини такомиллаштиш, инцидентларга нисбатан акс таъсир оперативлигини орттирилган тажрибани қўллаш орқали бир неча марта оширади. Ундан ташқари, бундай ёндошув ҳар томонлама ўрганилиши долзарб бўлган аномаль инцидентларни аниқлаш масаласини ҳал қилади.

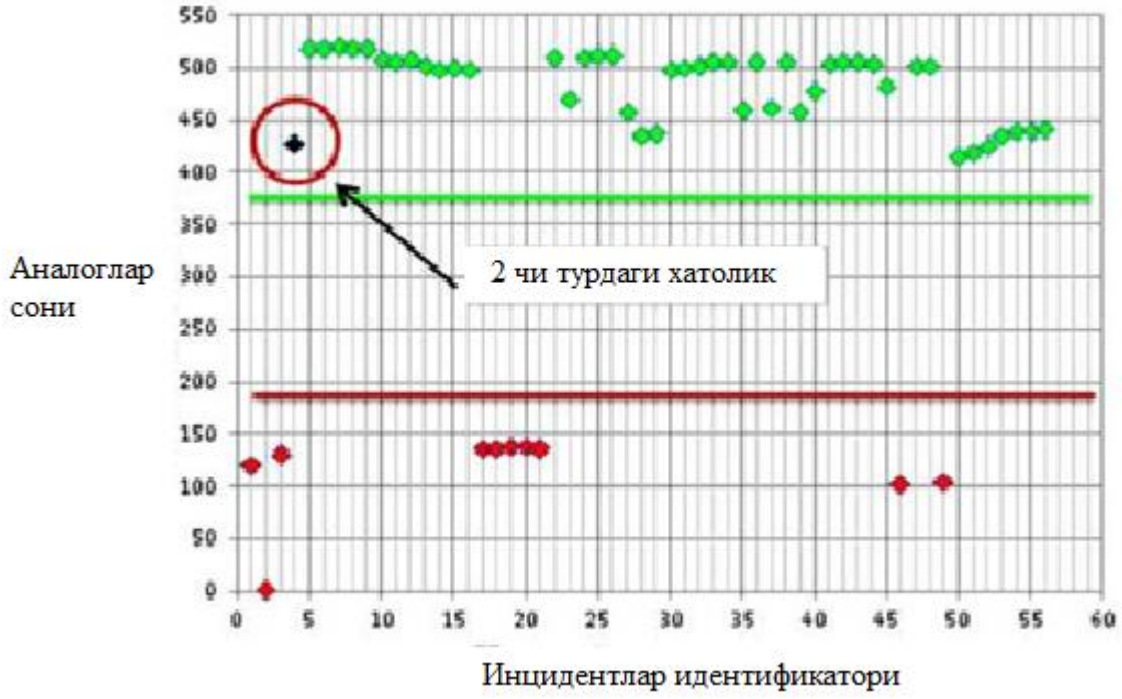
Рақамли экспериментлар натижалари. Алгоритмни бундай ечилиши натижани аналитик кўринишда, ҳам график нуқтали диаграмма кўринишида олиш имконини беради. Нуқтали диаграмма ёрдамида эътибор қаратилиши лозим бўлган инцидентларни - яъни аномал инцидентларни кўриш мумкин. (12.4-расм).



12.4-расм. Инцидентларни синфлаш натижалари

Кўриниб турибдики, нормал инцидентлар сифатида синфларга ажратилган инцидентлар, сон жихатидан кўпгина нормал инцидентлардан фарқ қилади, яъни ўхшашликлар сонини юқори қийматига яқинлашган. Бу ҳолат уларни ҳар томонлама таҳлил қилишни ва яширин сабабларни аниқлашни, инцидентлар натижасининг умумий қонуниятга буйсунмаслиги кўринади. Нуль гипотеза инцидентнинг нормаллигини таҳмин қилади, унда 1-турдаги хато нуль гипотезани нотўғрилигини инкор қилади, 2-турдаги хато нуль гипотезани нотўғри қабул қилинишидир. d_{lim} ва a_{lim} параметрларни

танлаш бир-бирига тескаридир. Бир томондан, аниқланган ўхшашликларнинг сонини ошиши синфлаш аниқлигини оширади(1-турдаги хатоларни камайтиради), лекин бунда синфлар орасидаги чегара унчалик аниқ бўлмайди. Орасидаги масофани камайиши аниқроқ синфлаштириш имконини беради, лекин 2-турдаги хатоликларни эҳтимоллигини оширади. (12.5-расм).



12.5-расм. Инцидентлар классификацияси натижалари

Кўриб турганимиздек бир нормал Инцидент нотўғри тасниф қилинди.

a_{lim} параметри муайян вазиятга боғлиқ. Таклиф қилинган Инцидентлар классификацияси

Прецедентли таҳлилнинг авзаллиги йиғилган тажрибани қайта қўллаш имконияти мавжудлиги ва ўхшаш инцидентлар учун акс таъсир сценарийси қидирув вақтини қисқаришидадир.

Таклиф этилган концепция муаммоли вазиятларда батафсил ўрганишни талаб етувчи ўхшаш инцидентларни аниқлашдек масалани ечиш ва прецедентлар базасида мавжуд бўлган билимлар асосида инцидентлар ечимни киритиш жараёнини автоматлаштириш имконини беради.

Ишни бажариш учун вазифа ва топшириқлар

1. Case-Based Reasoning (CBR) тушунчаси.
2. Прецедентли таҳлил жараёни.
3. Бошқариш жараёнини такомиллаштириш учун прецедентли таҳлилнинг қўллаш концепцияси.
4. Прецедентли таҳлил модели алгоритми.
5. Прецедентли таҳлил тизими архитеттураси.
6. Прецедентли таҳлил тизими модели ва архитектураси асосида дастурий

модуль ишлаб чиқиш.

Фойдаланилган адабиётлар

1. Постановление Президента Республики Узбекистан от 27 июня 2013 г. № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан» Собрание законодательства Республики Узбекистан, 2013 г., № 40, ст. 528.
2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012 year.
3. David Endler, Mark Collier. Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions. McGraw-Hill/Osborne © 2007 (574 pages).
4. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.
5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

V. МУСТАҚИЛ ТАЪЛИМ МАВЗУЛАРИ

“Ҳужум инцидентлари ва унга реакция” фани бўйича талабанинг мустақил таълими шу фанни ўрганиш жараёнининг таркибий қисми бўлиб, услубий ва ахборот ресурслари билан тўла таъминланган.

Талабалар аудитория машғулотларида профессор-ўқитувчиларнинг маърузасини тинглайдилар, мисол ва масалалар ечадилар. Аудиториядан ташқарида талаба дарсларга тайёрланади, адабиётларни конспект қилади, уй вазифаси сифатида берилган мисол ва масалаларни ечади. Бундан ташқари, айрим мавзуларни кенгроқ ўрганиш мақсадида қўшимча адабиётларни ўқиб рефератлар тайёрлайди ҳамда мавзу бўйича тестлар ечади. Мустақил таълим натижалари рейтинг тизими асосида баҳоланади.

Уйга вазифаларни бажариш, қўшимча дарслик ва адабиётлардан янги билимларни мустақил ўрганиш, керакли маълумотларни излаш ва уларни топиш йўлларини аниқлаш, интернетдан фойдаланиб маълумотлар тўплаш ва илмий изланишлар олиб бориш, илмий тўгарак доирасида ёки мустақил равишда илмий манбалардан фойдаланиб илмий мақола ва маърузалар тайёрлаш кабилар талабаларнинг дарсда олган билимларини чуқурлаштиради, уларнинг мустақил фикрлаш ва ижодий қобилиятини ривожлантиради. Шунинг учун ҳам, мустақил таълимсиз ўқув фаолияти самарали бўлиши мумкин эмас.

Уй вазифаларини текшириш ва баҳолаш амалий машғулот олиб борувчи ўқитувчи томонидан, конспектларни ва мавзуни ўзлаштириш даражасини текшириш ва баҳолаш эса, маъруза дарсларини олиб борувчи ўқитувчи томонидан ҳар дарсда амалга оширилади.

Талабалар мустақил таълимининг мазмуни ва ҳажми

№	Мустақил таълим мавзулари	Берилган топшириқлар	Бажариш муддати	Ҳажми (соатда)
I– семестр, 1- мустақил иш				
1	Ахборот хавфсизлиги инцидентлари мақсади ва вазифаси.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	1-ОН гача	4
2	Ахборот хавфсизлиги инцидентлари	Техник адабиётлар, Интернет	1-ОН гача	3

	сиёсатини қуриш.	материалларини йиғиш. Индивидуал топшириқларни бажариш		
3	Ахборот хавфсизлиги инцидентлари бошқариш тизимларини таҳлил этиш усуллари.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	1-ОН гача	4
4	Ахборот хавфсизлиги инцидентлари жараёнини бошқариш воситалари.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	1-ОН гача	2
5	Ахборот хавфсизлиги инцидентлари аниқлаш ва баҳолаш.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	1-ОН гача	3
6	Ахборот хавфсизлиги инцидентларида экспертиза жараёнини ўтказиш.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	1-ОН гача	2
7	Ахборот хавфсизлиги инцидентларига жавоб қайтариш ҳаёт даври процедураси таҳлил этиш.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	2-ОН гача	2
8	Ахборот хавфсизлиги инцидентларига жавоб қайтариш гурухларини шакллантириш.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	2-ОН гача	2
9	Ахборот хавфсизлиги инцидентларини	Техник адабиётлар, Интернет	2-ОН гача	3

	бошқариш дастурлари таҳлил этиш ва дастурий модуллар ишлаб чиқиш усуллари.	материалларини йиғиш. Индивидуал топшириқларни бажариш		
10	Ахборот хавфсизлиги инцидентлари ҳақида хабардор этиш механизмини тадқиқи.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	2-ОН гача	4
11	Ахборот хавфсизлиги инцидентларини тергов қилиш жараёнидаги қаршиликларни бартараф этиш усуллари.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	2-ОН гача	3
12	Криминалистик жиноятлар ва уларнинг классификацияси.	Техник адабиётлар, Интернет материалларини йиғиш. Индивидуал топшириқларни бажариш	2-ОН гача	4
Жами				**36**

VI. ГЛОССАРИЙ

Термин	Ўзбек тилидаги шарҳи	Инглиз тилидаги шарҳи
Ахборот	муайян объект хусусидаги билимларимизнинг ноаниқлик даражасини пасайтиришга имкон берувчи ҳар қандай маълумот.	data that reduces the uncertainty degree of knowledge about certain object.
Автоматлаштирилган ахборот тизими	маълумотларни ва ахборотни яратиш, узатиш, ишлаш, тарқатиш, сақлаш ва/ёки бошқаришга ва ҳисоблашларни амалга оширишга мўлжалланган дастурий ва аппарат воситалар.	a set of software and hardware designed for the creation, transmission, processing, distribution, storage and/or data and information management and production calculations.
Хавф-хатарни агрегирлаш	бирлашган хавф-хатарни теранрок тушунишга мўлжалланган бир неча хавф-хатарни битта хавф-хатарга бирлаштириш.	combine multiple risks in a risk, aimed at a better understanding of the overall risk.
Хавф - хатар тахлили	номувофик ҳодисалар пайдо бўлиш ҳолида кутиладиган зарарни аниқлаш мақсадида, эҳтимоллик ҳисоблашлардан фойдаланиб, тизим характеристикаларини ва салбий томонларини ўрганиш жараёни. Хавф – хатарни таҳлиллаш масаласи у ёки бу хавф – хатарнинг мақбуллик даражасини аниқлашдан иборат.	the process of studying the characteristics and weaknesses of the system, conducted using a probabilistic calculations in order to determine the expected damage in case of adverse events. The task of risk analysis is to determine the acceptability of a risk to the system.
Хавфсизлик хизмати маъмури	хавфсизликни таъминлашнинг бир ёки бир неча тизими ҳамда лойиҳалашни назоратлаш ва улардан фойдаланиш хусусида тўлиқ тасаввурга эга шахс (ёки шахслар гуруҳи).	person (or group of people) having (s) complete understanding of one or more security systems and controls (s) design and use.
Фаол тахдид	тизим ҳолатига атайин рухсатсиз ўзгартириш киритиш таҳдиди.	the threat of a deliberate unauthorized system state changes.
Трафик тахлили	1. Трафик оқимини кузатиш (борлиги, йуклиги хажми, йуналиши ва частотаси) асосида ахборат холати хусусида хулоса қилиш. 2. Дешифрланишга сабаб бўлмайдиган, аммо ғанимга ёки бузғунчига узатилаётган очик матн ва, умуман, кузатилаётган алоқа тизимининг ишлаши хусусидаги билвосита ахборотни олишига имкон берувчи алоқа	1 . Report on the state information based on observation of traffic flows (presence , absence, amount , direction and frequency . 2 . Analysis of all encrypted messages sent over the communication system does not lead to decrypt , but allowing the opponent and / or the offender obtain indirect

	тизими орқали узатилувчи шифрланган хабарлар мажмуининг таҳлили. Трафик таҳлили шифрланган хабарларнинг расмийлаштириш хусусиятларидан, уларнинг узунлиги, узатилиш вақти, узатувчи ва қабул қилувчи хусусидаги маьлумотлардан фойдаланади.	information about the transmitted Post and generally observed on the functioning of the communication system. A. that uses features of registration messages encrypted , and their length , the transmission time , the data sender and recipient , etc.
Тармоқ тахлиллагичлари (сниффер)	тармоқ трафигини “тинглаш”ни ва тармоқ трафигидан автоматик тарзда фойдаланувчилар исмини, паролларни, кредит карталар номерини, шу каби бошқа ахборотни ажратиб олишни амалга оширувчи дастурлар.	programs, asking for “listening” network traffic and automatically selects the network traffic of user names, passwords, credit card numbers, other similar information.
Аппарат ҳимоя	компьютерда маълумотларни ҳимоялашда аппарат воситалардан, масалан, чегара регистрларидан ёки қулфлардан ва калитлардан фойдаланиш.	the use of hardware, for example, registers boundaries or locks and keys to protect data in computers.
Фаол хужум	криптотизимга ёки криптографик протоколга ҳужум бўлиб, унга биноан душман ва/ёки бузғунчи конуний фойдаланувчи харакатига таъсир этиши, масалан, қонуний фойдаланувчи хабарини алмаштириши ёки йўқ қилиши ва хабарни яратиб унинг номидан узатиши ва ҳ. мумкин.	attack on a cryptosystem or cryptographic protocol in which the offender or the enemy and can affect the legitimate user actions, for example, replace or remove legitimate posts, create and send messages on his behalf, etc.
Хизмат қилишдан воз кечишга ундайдиган атайин қилинмайдиган ҳужум	тасодифий юз берган ҳолат натижасида (реклама натижасида қизиқишнинг кескин ошиши, тўсатдан ва кутилмаган камдан – кам бўладиган машҳурлик ва ҳ.) DOS ҳужумнинг мавaффақиятли ўтказилгани хусусида таассурот туғдирувчи қандайдир сервис учун хизмат қилишдан воз кечиш. Кўпинча фаолликнинг авж онларида янгилик сайтларига қизиқарли ахборотни жойлаштириш натижасида, хамда қидирув тизимлари ёрдамида оммабоп URL – ҳаволаларни ўтказиш қобилияти чекланган фойдаланиш каналларига эга медиа – ресурсларига индекслаш натижасида пайдо бўлади.	denial of service for any service which has come as a result of chance (sharply increased interest in the result of the promotion , the sudden and unexpected exception pop, etc.) , giving the impression of a successful DoS attack . Often occurs in times of peak activity as a result of placement of interesting information on news sites , as well as from popular search engines indexing URL- links to various media resources with limited bandwidth channel access.

Хавфсизлик аудити	компьютер тизими хавфсизлигига таъсир этувчи бўлиши мумкин бўлган хавфли ҳаракатларни характерловчи, олдиндан аниқланган ҳодисалар тўпламини рўйхатга олиш(аудит файлида қайдлаш) йўли билан ҳимояланишни назоратлаш.	maintain security control by registering (fixation in the audit file) a predetermined set of events that characterize the potentially dangerous actions in the computer affecting its security.
Ахборот тармоғи хавфсизлиги	ахборот тармоғини рухсатсиз фойдаланишдан, меъёрий ҳаракатига тасодифан аралашишдан ёки компонентларини бузишга уринишдан сақлаш чоралари.	measures designed to protect network information from unauthorized access, accidental or intentional interference with normal activities or attempts to destroy its components.
Компьютер тизими хавфсизлиги	деструктив ҳаракатларга ва ёлғон ахборотни зўрлаб қабул қилинишига олиб келувчи ишланадиган ва сақланувчи ахборотдан рухсатсиз фойдаланишга уринишларга компьютер тизимининг қарши тура олиш ҳусусияти.	property computer systems to resist attempts of unauthorized access to information processed and stored, the input of information, leading to destructive actions, and the imposition of false information.
Ходим хавфсизлиги	қандайдир жиддий ахборотдан фойдаланиш имкониятига эга барча ходимларнинг керакли авторизацияга ва барча керакли рухсатномаларга эгалик кафолатини таъминловчи усул.	method of ensuring that all personnel having access to some sensitive information has the necessary authorization, as well as all the necessary permissions.
Корхона хавфсизлиги	корхона ўз фаолиятини бузилишсиз ва тўхталишсиз юргиза оладиган вақт бўйича барқарор башоратланувчи атроф-муҳит ҳолати.	stable condition projected time environment in which the company can carry out their activities without disturbances and interruptions.
Ахборотнинг блокировка қилиниши	ахборотнинг техник воситалар ёрдамида ишланишида унинг фойдаланувчанлик хусусиятининг йўқолиши. Натижада танишиш, хужжатлаш, модификациялаш ёки йўқ қилиш бўйича ваколатли амалларни бажариш қийинлашади ёки тўхтатилади.	the loss of information when it is processed by technical means accessibility property, expressed in difficulty or termination of authorized access to it for authorized operations familiarization, documentation, modification, or destruction.
Хавф-хатарга таъсир	ҳавф-хатарни модификациялаш (ўзгартириш) жараёни. Ҳавф-хатарга таъсир қуйидагиларни ўз ичига олиши мумкин: фаолиятини бошламаслик ёки давом эттирмаслик қарори орқали хавф-хатарни олдини олиш натижасида хавф-хатар пайдо бўлади; қулай имкониятдан	the modification (changing) risk. Effects on risk may include: - avoid the risk by decision not to commence or to continue, resulting in the risk; - Adoption or increase the risk for a favorable opportunity; - Eliminate the source of the risk; - Changing

	фойдаланиш учун хавф-хатарни қабул қилиш ёки кўпайтириш; хавф-хатар манбаини йўқ қилиш; имкониятини ўзгартириш; оқибатларни ўзгартириш; хавф-хатарни бошқа тараф ёки тарафлар билан бўлишиш (жумладан, шартномалар ва хавф-хатарни молиялаш); хавф-хатарни тушунган ҳолда ушлаб қолиш.	opportunities; - Change impacts; - Sharing the risk with another party or parties (including contracts and risk financing); - Conscious retention risk.
Конфиденциаль ахборотдан фойдаланиш	муайян шахсга таркибида конфиденциаль характерли маълумот бўлган ахборот билан танишишга ваколатли мансабдор шахснинг рухсати.	authorized authorized official introduction of a particular person with the information containing confidential information.
Ахборотдан рухсатсиз фойдаланиш	манфаатдор субъектнинг ҳуқуқий ҳужжатларни ёки мулкдор, ахборот эгаси томонидан ўрнатилган ҳимояланувчи ахборотдан фойдаланиш ҳуқуқлари ёки қоидаларини бузиб ҳимояланувчи ахборотга эга бўлиши.	preparation of protected information interested entity in violation of the legal instruments or by the owner, the owner of the information or rights of access to protected information.
Тизимнинг осилиб қолиши	янги топшириқлар киритилишини бостириш йўли билан мультидастур тизимини тўхтатиш (“яхлатиш”).	system hang - stop ("freezing") multiprogramming system by inhibiting the entry of new jobs.
Ахборотни фош қилинишдан ҳимоялаш	ҳимояланувчи ахборотни, ушбу ахборотдан фойдаланиш хуқуқига эга бўлмаган манфаатдор субъектларга (истеъмолчиларга) рухсатсиз етказишни бартараф этишга йўналтирилган ахборот ҳимояси.	the information security directed on prevention of unauthorized finishing of protected information to interested subjects (consumers), not having right of access to this information.
Ижтимоий инженерия	хизматчи ходимлар ва фойдаланувчилар билан, турли найранг, алдаш ва ҳ. орқали чалғитиш асосидаги мулоқотдан олинадиган ахборот ёрдамида ахборот тизимининг хавфсизлик тизимини четлаб ўтиш.	round of system of safety of system information by means of information received from contacts with the service personnel and users on the basis of their introduction in delusion at the expense of various tricks, deception and so forth.
Инсайдер	гурухга тегишли яширин ахборотдан фойдаланиш хуқуқига эга гурух аъзоси. Одатда, ахборот сирқиб чиқиш билан боғлиқ можорода муҳим шахс ҳисобланади. Шу нуқтаи	the member of group of the people having access to the classified information, belonging this group. As a rule, is the key character in the incident, connected with

	назаридан, инсайдерларнинг қуйидаги хиллари фарқланади: бепарволар, манипуляцияланувчилар, ранжиганлар, қўшимча пул ишловчилар ва ҳ.	information leakage. From this point of view distinguish the following types of insiders: negligent, manipulated, offended, disloyal, earning additionally, introduced, etc.
Инцидент	рухсатсиз фойдаланиш хуқуқига эга бўлишга ёки компьютер тизимига хужум ўтказишга уринишнинг қайд этилган холи.	the recorded case of attempt of receiving unauthorized access or carrying out attack to computer system.
Ташқи инцидент	манба жабрланувчи томон билан бевосита боғланмаган бузғунчи бўлган можоро.	the incident which source is the violator who hasn't been connected with an affected party directly.
Ички инцидент	манба жабрланувчи томон билан бевосита боғланган (меҳнат шартномаси ёки бошқа усуллар билан) бузғунчи бўлган можоро.	the incident which source is the violator connected with an affected party directly (the employment contract or other ways).
Ахборотдан ноқонуний фойдаланиш	қонуний йўл билан олинган маълумотларни, ушбу маълумотларга ва бундай ҳаракатларга қўл урувчи субъектларга ўрнатилган қоидаларни ва ваколатларни (санкцияларни) бузган ҳолда, узатиш, тарқатиш (чоп этиш) ва қўллаш.	transmission, distribution(publishing), the use of information obtained through legal means in violation of the rules and powers(sanctions) established forthis information and subject,to take such action.
Суқилиб киришга синаш	тизимни унинг ҳимоялаш воситасини (хусусан, рухсатсиз фойдаланишдан ҳимоялаш воситасини) текшириш мақсадида синаш.	system test for the purpose of check of means of its protection (in particular from illegally го access).
Яширин канал	хавфсизлик сиёсатини бузиш учун ишлатилиши мумкин бўлган, ахборот технологияси тизимини ва автоматлаштирилган тизимларни ишлаб чиқарувчилар кўзда тутмаган коммуникация канали. Ахборот узатиш механизми бўйича яширин каналлар хотира бўйича яширин каналга, вақт бўйича яширин каналга ва статистик яширин каналга бўлинади.	unforeseen the developer of system of technologies information and systems automated the communication channel which can be applied to security policy violation. On the information transfer mechanism c.s subdivide on: c.s. on memory c.s. on time; hidden statistical channels.
Ахборот сирқиб чиқувчи канал	кўрикланувчи маълумотлардан (тижорат сири, физик муҳит ва саноат айғоқчилик воситалари мажмуи) рухсатсиз фойдаланишга имкон берувчи	actual path from a source of confidential information to the malefactor, on which probably unauthorized obtaining protected data (set of a source

	конфиденциаль ахборот манбаидан то нияти бузуқгача бўлган физик йўл.	of a trade secret, the physical environment and means of industrial espionage).
Кейлоггер	клавиатурали киритишни ушлаб қолишга мўлжалланган дастур ёки аппарат восита. Босилган клавишлар скан-кодларини аниқлашни ва уларни яширинча сақлашни ва/ёки яширинча қандайдир канал орқали узатишни амалга оширади.	the program or the hardware device intended for interception of keyboard input. Carries out recognition of scan-codes of the pressed keys and the hidden preservation and/or their hidden transfer on any channel.
Компьютер жиноятчилиги	ўзи ёки учинчи шахс учун мулкий фойда олиш ҳамда рақибига мулкий зиён етказиш мақсадида ахборот ресурсидан рухсатсиз фойдаланишни, уни модификациялашни ёки йўқотишни амалга ошириш.	implementation of unauthorized access to information resource, its modification (fake) or destruction for the purpose of obtaining property benefits for itself or for the third party, and also for causing property damage to the competitor.
Мантиқий “бомба”	ахборотдан рухсатсиз фойдаланиш учун маълум вақтий ва ахборот шароитларида ишга туширилувчи дастур.	the program which is started under certain temporary or information conditions for implementation of unauthorized access to information.

VII. АДАБИЁТЛАР РЎЙХАТИ

Асосий дарсликлар ва ўқув қўлланмалар рўйхати

1. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия–Телеком, 2014. – 170 с.

2. Joe Fichera and Steven Bolt. «Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response». 2012.

3. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

4. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012.

Қўшимча адабиётлар

1. 2017-2021 йилларда ўзбекистон республикасини ривожлантиришнинг бешта устувор йўналишлари бўйича ҳаракатлар стратегияси, Ўзбекистон Республикаси Президенти Ш.М. Мирзиёевни 7-апрелда имзоланган фармони.

2. Мирзиёев Ш.М. Эркин ва фаровон, демократик Ўзбекистон давлатини биргаликда барпо этамиз. 2017.

3. Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. 2017.

4. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». – М.: Стандартинформ, 2009. – 50 с.

Интернет сайтлари

1. Зиёнет ахборот-талим портали. http://www.ziyonet.uz

2. https://infosec.uz/uz/incidents/344/

3. http://uzcert.uz/report/

4. http://www.hbc.ru/news/analytics/security

5. http://itsecurity.ru/catalog/bezopasnos-informatsionnyh-tehnologiy