

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АЛОҚА, АХБОРОТЛАШТИРИШ ВА
ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚЎМИТАСИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Қўл ёзма ҳуқуқида

УДК 004.75

АЛЛАНОВ ОРИФ МЕНГЛИМУРАТОВИЧ

Интернет магазинда ҳимояланган электрон тўловларни ташкил этиш

5А330302 – Ахборот хавфсизлиги

Магистр академик даражасини олиш учун ёзилган
диссертация

Илмий раҳбар:

Қодиров А.А.

Тошкент – 2014

МУНДАРИЖА

	Кириш	5
I боб.	Электрон тижорат хавфсизлиги	10
	1. Ананавий ва электрон тижорат	10
	2. Электрон тўлов тизимлари	19
	3. Ананавий тижорат тўлов тизимларида хавфсизлик	26
	4. Электрон тижорат хавфсизлиги	29
	5. Ўзбекистонда мавжуд электрон тўлов тизимлари	37
	I боб бўйича хулосалар	42
II боб.	Электрон тўлов тизимларида хавфсизликни таъминлаш	43
	1. Электрон тўлов тизимида хавфсизлик масаласи	43
	2. B2C ва C2C тизимларида электрон транзакция хавфсизлиги	45
	3. Электрон тўлов стандартлари таҳлили.....	62
	II боб бўйича хулосалар	70
III боб.	Интернет магазинда тўлов тизими хавфсизлигини таъминлаш	71
	1. Электрон тўлов тизимининг криптографик ҳимоя воситалари таҳлили	71
	2. Интернет магазин тизимини яратиш	78
	3. Интернет-магазинда хавфсизликни таъминлаш	82
	III боб бўйича хулосалар	92
	Хулоса	94
	Фойдаланилган адабиётлар	95
	Илова.....	98

КИРИШ

Диссертация мавзусининг асосланиши ва унинг долзарблиги. “XXI аср – ахборот технологиялари асри” - деб бежизга айтмаганлар Президентимиз И. А.Каримов. Бу аср остида одамзот тасаввур қила олмаган сунъий интеллект роботлари, технологиялар ва бошқа техник қурулмалар яратилишига ҳеч ким шубҳа қилмаса керак. Ахборот технологияларни ривожланиши ҳар бир мамлакат учун иш унумдорлигини ошиши, сифати ва энг асосийси иш самарадорлиги юқори даражада бўлишини таъминлаб беради. Ўзбекистон Республикаси мустақиллик йиллари ахборотлаштириш соҳасида инқилобий ўзгаришлар даврини бошдан кечирмоқда. Замонавий ахборот-коммуникация технологиялари қулайликлар яратиш билан бир қаторда янги муаммоларни ҳам ўртага қўймоқда.

Мустақиллик йиллари мамлакатимизда ахборот телекоммуникация технологияларининг жадал суръатлар билан ривожланиб бориши глобал ахборот жамиятида Ўзбекистон Республикаси ҳам муносиб ўрин эгаллашига катта таъсир кўрсатди.

Ҳозирги кунда ахборот базаларида сақланаётган ва телекоммуникация тизимларида айланаётган ахборот хавфсизлигига таҳдид кескин ошиб бормоқда. Натижада ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди.

1974-йилда ўзбек олими Ўзбекистонда хизмат кўрсатган фан арбоби, профессор Хасанов Пўлат Фаттохович томонидан таклиф етилган диаматрицалар алгебрасини марказимиз директор ўринбосари Хасанов Хислат Пўлатович томонидан криптография масалаларини ечиш учун такомиллаштирилиб топилган параметрли алгебра ишлаб чиқилди. Бунинг натижасида Фан-техника ва маркетинг тадқиқотлари марказининг бош илмий ходими Хасанов П. Ф. раҳбарлигида 2002-йилда криптография бўйича биринчи патентга талабнома берилди. Бу патент 2006-йилда Ўзбекистон Республикаси давлат патент идораси томонидан рўйхатга олинди ва

“Рақамли имзони шакллантириш ва аутентификация усули” ихтироси учун 03070-сонли патент берилди.

03070-сонли “Рақамли имзони шакллантириш ва аутентификация усули” патенти ғоялари Фан-техника ва маркетинг тадқиқотлари маркази ходимлари томонидан ишлаб чиқилган Ўзбекистон Республикасининг криптография соҳасидаги дастлабки давлат стандартларига асос бўлди. О`з DSt 1092:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси, Электрон рақамли имзони шакллантириш ва текшириш жараёнлари”, О`з DSt 1105:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми”, О`з DSt 1106:2009 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси” шулар жумласидандир. Криптография йўналишини ривожлантиришга давлатимиз томонидан ҳам катта аҳамият берилмоқда. Бунга кейинги йилларда қабул қилинган бир нечта қонун ва меъёрий ҳужжатлар, жумладан, “Электрон рақамли имзо”, “Электрон ҳужжат айланиши” тўғрисидаги қонунлар, Президентимизнинг 2007-йил 3-апрелда қабул қилган “Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил етиш чора-тадбирлари” тўғрисидаги қарори мисол бўлиши мумкин.

03070-сонли “Рақамли имзони шакллантириш ва аутентификация усули” патенти ғоялари Ўзбекистон Республикасининг қонун ва қарорларини амалга татбиқ етишда муҳим аҳамият касб етмоқда. Сўнгги йилларда миллий стандартларга асосланиб е-НУЈЈАТ - электрон ҳужжат алмашиш тизими, е-ХАТ электрон хат алмашиш тизими, ҳимояланган файл “НІМФАУЛ” тизими ва масофавий солиқ ҳисоботи топшириш тизими учун криптопровайдерлар ишлаб чиқилди. Ўзбекистон Республикасининг миллий криптографик алгоритмларини яратиш, уларни такомиллаштириш ва ахборотни криптографик муҳофазалашнинг миллий дастурий ва аппарат-дастурий воситаларини ишлаб чиқиш Ўзбекистон Республикаси Президентининг 2007 йил 3-апрелдаги “Ўзбекистон Республикасида ахборотнинг криптографик

муҳофазасини ташкил етишга оид чора-тадбирлар тўғрисидаги” 614-сонли қарорида биринчи галдаги вазифа қилиб қўйилганлигини ҳисобга олсак, мазкур ихтиро бу қарорнинг бажарилишини таъминлашда муҳим аҳамиятга эгадир.

Интернет тармоғини ҳаётимизнинг барча соҳаларида кириб келиши натижасида қатор имкониятлар юзага келмоқда. Булардан ҳозирда кенг ривожланётгани интернет орқали тўлов хизматидир. Ҳозирда онлайн тўлов тизимини қўллаб-қувватловчи интернет магазинлар интернет тармоғида кенг ривожланмоқда.

Ушбу соҳани ривожлантириш ва ҳимоялаш мақсадида Ўзбекистон Республикаси Марказий банки томонидан қуйидаги қонуний ҳужжатлар ишлаб чиқилди:

- Ўзбекистон Республикаси "Ўзбекистон Республикасининг Марказий банки тўғрисида"ги Қонуни (21.12.1995 й., № 154-І);
- Ўзбекистон Республикаси "Банклар ва банк фаолияти тўғрисида"ги Қонуни (25.04.1996 й., № 216-І);
- Ўзбекистон Республикаси "Электрон тўловлар тўғрисида"ги Қонуни (16.12.2005 й., № ЎРҚ-13);
- "Марказий банкнинг банклараро тўлов тизими орқали электрон тўловларни амалга ошириш тартиби тўғрисида"ги Низом (14.02.2006 й., № 1545);
- "Ўзбекистон Республикасида нақд пулсиз ҳисоб-китоблар тўғрисида"ги Низом (03.06.2013 й. № 2465).

Онлайн тўловлардан кенг фойдаланиш, интернет магазин хизматларидан фойдаланиш кўплаб имкониятлар ва қулайликлар берса, ўз ўрнида ушбу тизимда мавжуд камчиликларни бартараф этиш долзарб муаммолигини келтириб чиқаради.

Илмий тадқиқот ишининг объекти ва предметининг белгиланиши. Тадқиқотнинг объекти онлайн тўлов хизматини ўзида акс эттирган интернет магазин ҳисобланади.

Интернет магазин хизматини куриш тизими, унда тўлов тизими хавфсизлиги таъминлаш усуллари тадқиқотнинг предмети ҳисобланади.

Илмий тадқиқот ишининг мақсади ва вазифалари. Ушбу магистирлик диссертациясида олиб борилган илмий тадқиқот ишининг мақсади яратилган интернет магазин тизимида онлайн тўлов хавфсизлигини таъминлаш.

Тадқиқот мақсадини амалга ошириш учун диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

- Мавжуд онлайн тўлов тизимларини таҳлил қилиш;
- Интернет магазин ташкил этиш тизимини тадқиқ этиш;
- Онлайн тўлов тизими хавфсизлигини таъминлаш методлари таҳлили;
- Интернет магазин тизимини яратиш ва унда хавфсизликни таъминлаш.

Илмий тадқиқотнинг асосий масалалари ва фаразлари. Онлайн тўлов тизимидаги мавжуд камчиликларни таҳлил этган ҳолда, интернет магазинда тўлов хизмати хавфсизлигини таъминлаш.

Мавзу бўйича қисқача адабиётлар таҳлили. Интернет тармоғининг ҳаётимизда кириб келиши ва унда электрон тўловни амалга оширилиши ушбу тизимда ахборот хавфсизлигини таъминлаш долзарб муаммо эканлигини англатади.

Электрон тўлов тизимида ҳозирда катта молиявий ташкилотлар орасида келишув ва шартнома асосида стандартлар ишлаб чиқилиб, улар асосида тўлов амалга оширилмоқда. Ушбу корпорациялар орасида Visa ва MasterCard алоҳида мавқега эга.

Булардан ташқари Интернет копрацияси Google, мобиль алоқа операторлари w-НА ва мобиль восита ишлаб чиқарувчи ташкилотлар Ericsson ва BlackBerry ўртасида янги мобиль тўлов тизими ишлаб чиқилмоқда.

Илмий тадқиқот ишида қўлланилган услубларнинг қисқача тавсифи. Ушбу илмий тадқиқот ишида ахборотни криптографик ҳимоялаш тизимлари назарияси, эҳтимоллар назарияси, сонлар назарияси, математик

мантиқ ва комбинаторика методларидан фойдаланилган. Булардан ташқари солиштириш, тестлаш ва қиёсий таҳлил усулларида фойдаланилди.

Тадқиқот натижаларининг назарий ва амалий аҳамияти. Мавжуд онлайн тўлов тизими усуллари таҳлил этиш, интернет магазин ташкил этиш усуллари таҳлили, интернет магазинни яратиш алгоритмлари тадқиқи, криптографик ҳимоя усуллари асосида онлай тизим хавфсизлигини таъминлаш магаистрлик диссертация ишининг назарий аҳамияти саналади.

Магистрлик диссертациясининг амалий аҳамияти –таклиф этилган ҳимоя усуллари қўллаган ҳолда интернет магазин тизимини яратишдир.

Илмий тадқиқот ишининг илмий янгилиги. Ушбу тадқиқот ишининг янгилиги интернет магазинда мавжуд тўлов тизимларини таҳлил этиб, янги ҳимояланган тўлов тизими архитектурасини таклиф этиш.

Диссертация таркибининг қисқача тавсифи. Ушбу тадқиқот иши қуйидаги: кириш, 3 та бўлим, хулоса, фойдаланилган адабиётлар рўйхати ва иловадан иборат. Ушбу тадқиқот ишида 13 та жадвал, 30 та расмдан иборат. Илмий тадқиқот ишининг умумий ҳажми 97 саҳифани ташкил этади.

I боб. Электрон тижорат хавфсизлиги

1. Ананавий ва электрон тижорат

Маҳаллий бозорнинг жаҳон сармоя бозорига уйғунлашуви, бевосита хорижий инвестицияларни иқтисоднинг муҳим тармоқларига жалб қилиш ва иқтисодий ислоҳатлар жараёнини чуқурлаштириш яқин келажакда ҳал қилиниши лозим бўлган долзарб вазифадир. Ихтисослаштирилган ташкилотлар ва инвестиция институтлари хорижий инвесторларни Республика фонд бозорига жалб қилиш устида мунтазам иш олиб борилмоқда. Бу уйғунлашув икки ёқлама жараён бўлиб, хорижий фонд бозорларида Ўзбекистонлик инвесторлар фаолиятини ташкил этиш унинг муҳим қисмидир.

Бугунги кунда жаҳон фонд бозорининг кун сайин глобаллашуви, алоқа ва технологиялар ўзаро боғлиқликда ривожланиши инвесторнинг ўз маҳаллий дойрасида чекланиб қолмаслигига олиб келди. У эндиликда ўз сармоясини фойдалироқ жойлаштиришга ҳаракат қилади. Фонд бозори самарадорлиги юқори бўлган корхоналарни излайди ва бу билан маълум бир корхоналарнинг етакчилиқ ўрнини доймий равишда муҳофаза қилиб, белгилаб беради. Бирор корхонанинг кўрсаткичи пасайиши билан пуллар бозорнинг янги корхоналарига оқа бошлайди. Бу жараён узликсиз давом этади. Жаҳоннинг барча фонд бозорлари шу функцияни бажарадилар.

Замонавий компьютер технологиялари ҳар бир бақувват инвесторга Интернет орқали йирик фонд бозорлари фаолиятида иштирок этиш имкониятини яратмоқда. Инвестор брокерларни четлаб ўтган ҳолда кам сарф харажатлар билан барча зарур ахборотларни олиш ва акцияларни мустақил равишда ўзи харид қилиши ва сотиши мумкин. Саноати ривожланган давлатлар қимматли қоғозлар бозорида жуда яхши ташкил этилган ва юксак технологияли савдо жараёнини таъминлай оладиган даражада ривожланган инфратузилмага эга.

Ахборот хизматларининг ривожланиши, бозор ҳақидаги маълумотлар ҳаққонийлиги ва ишочилигини ҳам оширади. Бу эса ўз навбатида, қимматли

коғозлардан фойда олишга интилаётган янги-янги инвесторларни бозорга жалб қилади. Интернет томонидан тақдим этилаётган имкониятлар фақат бу жараёнларнигина тезлаштириб қолмай, балки уларни сифати жиҳатидан ҳам ўзгартирди.

Интернет ҳақиқатдан ҳам молиявий транзакциялар ва инвестициялар учун глобал тақсимловчи муҳитга айланиб бормоқда, аппаратлар ва дастурларнинг минимал захиралари мавжуд бўлган шароитда ҳам дунёнинг турли бурчакларидан унга осонгина кириш мумкин бўлиб қолмоқда. АҚШ юксак технологияли компанияларининг акциялар билан амалга оширадиган операциялари молия дунёсида тан олинган.

Маълумки, жаҳоннинг йирик банклари, траст компаниялари, нафақа фондлари ва брокерлик фирмалари ўз маблағларини айнан шундай акцияларга қўядилар. Бу акциялар билан ўтказиладиган операциялардан тушадиган фойдадан банклар ва бошқа молиявий ташкилотлар ўз мижозларига уларнинг қўйилмалари бўйича фоизларни тўлайдилар, бунда фойданинг бир қисмини ўзларига қолдирадилар. Фойда олишда юқори кўрсаткичларга эришиш учун жиддий ишлаш лозим, аввало, аҳволни яхши тушуна билиш ва бозорни танланган тармоқни ҳамда иқтисоднинг умумий ҳолатини синчковлик билан кузатиб бориш зарур. Асосийси, акциялар курсига ҳал қилувчи таъсир кўрсатадиган маҳаллий ҳодисалар тўғрисидаги вақтида хабардор бўлиш ва уларни таҳлил қилишни ўрганиш лозим. Мамлакатимиз барқарар бозор иқтисоди тизимига эга, эркин жамиятни қуришга интилмоқда. Валютани тартибга солиш ва хорижий инвестицияларни жалб қилишни такомиллаштиришга йўналтирилган қорорлар шундан далолат беради.

2001-йил 23 Майда Ўзбекистон Республикаси Вазирлар Маҳкамаси “2001-2005 йилларда компьютер ва ахборот технологияларини ривожлантириш, Интернетнинг халқаро ахборот тизимига кенг кириб боришини таъминлаш дастурини ишлаб чиқишни ташкил этиш чора тадбирлари” тўғрисида қарор қабул қилди. Унда замонавий ахборат

технологияларини иқтисодиёт, фан ва таълимнинг барча соҳаларига кенг жорий этиш, халқаро ахборот тизимларига, шу жумладан Интернетга кириб боришни кенгайтириш, юқори мақлакали дастурчи-мутахассислар тайерлаш даражасини ошириш мақсадида марказ ташкил қилиш таъкидлаб ўтилди. Ушбу қарорга асосан, фонд бозорида Интернет тармоғини ривожлантириш, кучли мутахассисларни жалб қилиш ва олди-сотди операцияларини амалга ошириш, биринчи галдаги вазифа қилиб қўйилди.

Қимматли қоғозлар бозорида операцияларда иштирок этаётган ҳар бир малакали мутахассис, брокер, эмитент, инвестор техниканинг илғор соҳаларидан фойдаланишига тўғри келади. Бу эса ўз минжозлари сонини купайтиришга, сифатли ахборотларни ўз вақтида етказиб беришда кенг имкониятларни очиб бермоқда. Айниқса, молия бозорининг шоҳобчаси бўлган қимматли қоғозлар бозорида рақобатбардош муҳитнинг яратилиши бозорнинг янада ривожланиши учун катта ҳиссасини қўшади. Бу турдаги ахборотларни ўз вақтида ва сифатли етказиб бериш республикамиздаги фонд бозорининг ривожланишида ҳам муҳим аҳамиятга эга. Молия бозорида операцияларни амалга ошириш жааёнида зудлик билан ахборотларни қабул қилиш, имкониятлардан фойдаланиб инвестиция лойиҳаларини ишлаб чиқиш, ҳар қандай эҳтимолий хатоларнинг олдини олиш, хатарли муносабатлар таъсир дойрасини камайтириш “тўғридан-тўғри” қарор қабул қилиш ҳар доим ҳам кутилаётган, кўзланаётган натижани бермайди. Юқорида кўриб ўтилган муносабатларни янада жадаллаштириш, вақтдан унумли фойдаланиш мақсадида, кўпгина ривожланган давлатларда Интернет тармоғидан фойдаланиш йўлга қўйилмоқда.

Банклар қимматли қоғозларни сотишда ёки сотиб олишда асосий воситачи сифатида муҳим роль ўйнайди. Шунингдек, банклар қимматли қоғозларни сотишда брокер сифатида қатнашиб, ишларни сифатли олиб бориш, вақтдан унумли фойдаланиш, мижозларга ахборотларни ўз вақтида етказишда ҳам асосий ўрин тутаяди. Бу жараёнларни янада такомиллаштиришда Интернет банклар муҳим аҳамиятга эга бўлиб,

Интернет иқтисод тушунчаси бугутги кунда ҳар қандай соҳанинг ажралмас қисми бўлиб қолди. Ривожланган мамлакатлар банклари ўз хизмат даражаларини кенгайтирган ҳолда миждозларига Интернетдан фойдаланишнинг энг маъқул йўллари тавсия қилмоқдалар. Бугунги кунда банк соҳасида e-banking янги термини пайдо бўлди еки Интернет-банк тармоғи юзага келди.

Техника воситаларидан, ахборот технологияларидан ва ахборот тизимлари хизматларидан фойдаланган ҳолда электрон тўлов ҳужжатлари воситасида нақд пулсиз ҳисоб-китобларни амалга ошириш электрон тўловдир.

Электрон тўлов тизимида товарлар(хизматлар) тўлови харидорнинг электрон ҳисобидан шахсий банк рақами ҳисобига пул маблағларини чиқариш имконига эга бўлган сотувчининг электрон ҳисобига пул маблағларини ўтказиш йўли билан амалга оширилади.

Электрон тижорат Интернет тармоғидаги тижорат соҳасига оид фаолликни, унда олди-сотдини амалга оширилишини ифодалаш учун қўлланилади. У компьютер тармоғидан фойдаланган ҳолда харид қилиш, сотиш, сервис хизмати кўрсатишни амалга ошириш, маркетинг тадбирларини ўтказиш имкониятини таъминлайди.

Электрон тижорат – бу тижорат алоқаларининг бир тури бўлиб, сотувчи ва харидор уртасидаги шартномалар ҳамда хизматлар Интернет орқали амалга оширилади.

Интернетда турли компаниялар ўз товар ва хизматларини реклама қиладилар. Улар бу ишни Интернетда жойлашган электрон каталоглар ёрдамида амалга оширадилар. Электрон каталогларда товар ва хизматлар ҳақида тўлиқ маълумотлар келтирилади: товар номи, ишлаб чиқарилган сана, кўриниши, тури, савдо тури, нархи, транспорт харажатлари, миждозларнинг бурчлари, суғурта ва етказиб бериш шартлари акс эттирилади.

Электрон тижорат фаолияти Ўзбекистон Республикасининг “Электрон тижорат тўғрисида”ги 2004 йил 29 апрелдаги 613-II сон Қонуни билан белгиланади ва амалга оширилади[5].

Электрон тижоратнинг анъанавий савдо туридан қуйидаги характерли хусусиятлари билан фарқланади:

- харидор ўзига қулай вақт, жой ва тезликда маҳсулотни танлаш ва сотиб олиш имкониятига эга;
- савдо-сотиқ фаолиятини иш фаолияти билан бирга параллел равишда, яъни ишлаб чиқаришдан ажралмаган ҳолда олиб бориш имконияти мавжуд;
- кўп сонли харидорларнинг бир вақтнинг ўзида бир нечта фирмаларга мурожаат қила олиши. Бу кўп сонли харидорларнинг алоқа воситалари ёрдамида сотувчилар билан мулоқотда бўлиш имконияти;
- керакли маҳсулотларни тезликда излаб топиш ва шу маҳсулотлари бор фирмаларга мурожаат қилишда техника ва транспорт воситаларидан самарали фойдаланиш, маҳсулотларни бир жойга йиғиш ва уларни сотиб олишда аниқ манзилларга мурожаат қилиш. Ортиқча вақт ва харажатларни камайтиради;
- харидорнинг яшаш жойи, соғлиғи ва моддий таъминланиш даражасидан қатъий назар ҳамма қатори тенг ҳуқуқли маҳсулот сотиб олиш имконияти;
- ҳозирги кунда чиққан жаҳон стандартларига жавоб берадиган маҳсулотларни танлаш ва сотиш имконияти;
- электрон тижорат сотувчининг маҳсулотларини (иш, хизматларини) сотиш жараёнидаги имкониятини янада кенгайтиради ва янгилайди. Энди сотувчи маҳсулотларини сотиш жараёнини тезлаштириши, янги ва сифатли маҳсулотларни мунтазам алмаштириши, маҳсулотларнинг айланма ҳаракатини тезлаштириши керак бўлади.

Электрон тижоратда савдони ташкил қилиш фирмаларнинг рақобатини кучайтиради, монополиядан чиқаради ва маҳсулотларнинг сифатини ошириш

имкониятини беради. Харидорлар кундалик ҳаётида керакли маҳсулотлар ичида сифатлиларини танлаши мумкин. Чет эл фирмаларига мурожаат қилади.

Электрон пул – бу пул бирлигига тенглаштирилган белгилар ҳамда купюра ва танга ролини бажарувчи жуда катта сон ёки файллардир. Бундай тизимнинг фаолият кўрсатиш харажатлари бошқаларидан анча кам. Бундан ташқари, электрон пуллар тўлиқ анонимликни таъминлаши мумкин, чунки уни ишлатган мижоз ҳақида ҳеч қандай маълумот берилмайди[19].

Электрон пул birlikлари қуйидагилар:

WMY – Ўзбекистон зонасида операцияларни амалга ошириш учун UZSнинг Y-ҳамёндаги эквиваленти.

WMR – рубль зонасида операцияларни амалга ошириш учун RURнинг R-ҳамёндаги эквиваленти, WMR операцияларининг кафили бўлиб WebMoney Transfer нинг Россия ҳудудидаги вакили “БМП” МЧЖ хизмат қилади.

WMZ – АҚШ долларида операцияларни амалга ошириш учун USD нинг Z-ҳамёндаги эквиваленти.

WME – EBPO да операцияларни амалга ошириш учун EURнинг E-ҳамёндаги эквиваленти, WMZ ва WME операцияларининг кафили бўлиб Amstar Holdings Limited, S.A. хизмат қилади.

WMU – Украина зонасида операцияларни амалга ошириш учун UANнинг U-ҳамёндаги эквиваленти, WMU операцияларининг кафили бўлиб “Украинское Гарантийное Агентство” МЧЖ хизмат қилади.

WMB – Беллорусия зонасида операцияларни амалга ошириш учун BYRнинг B-ҳамёндаги эквиваленти.

WMG – 1 грамм олтиннинг G-ҳамёндаги эквиваленти.

WBC ва WMD – WMZнинг C ва D ҳамёнлардаги кредит операциялари учун эквиваленти.

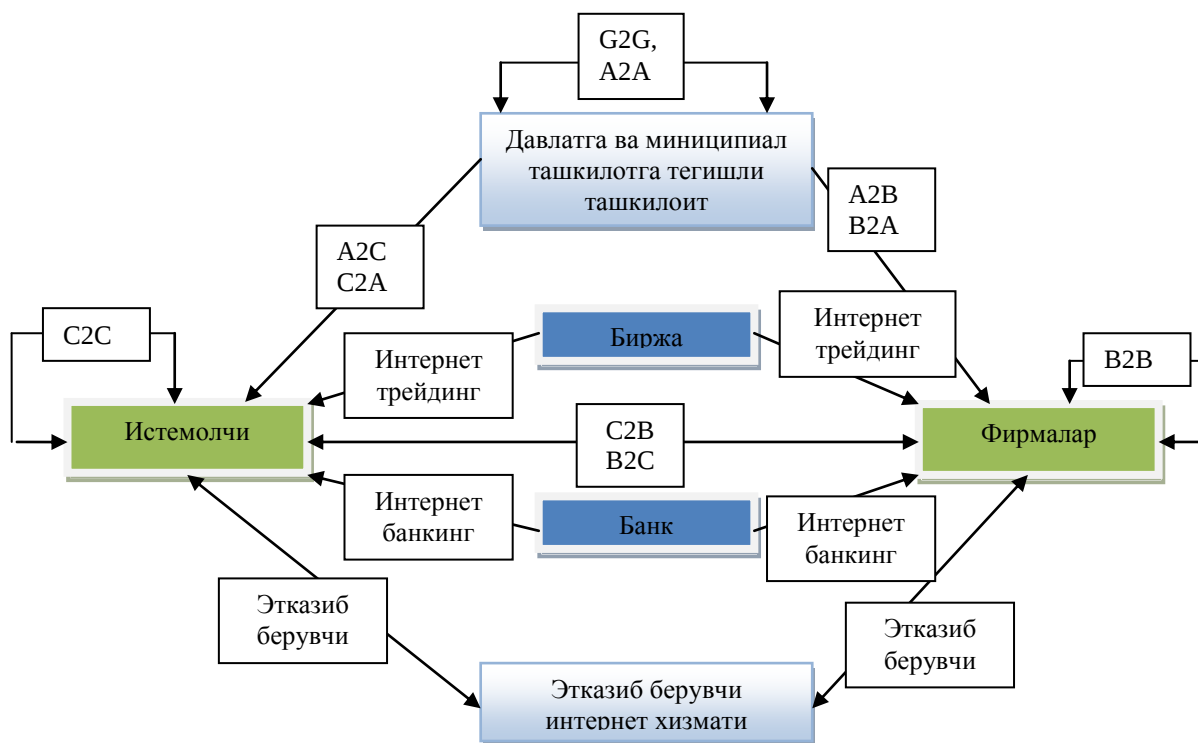
Интернет тармоғида электрон тижрат моделлари қуйидагича[17]:

- B2C (Business-to-Consumer) — "фирма—истемолчи";
- B2B (Business-to-Business) — "фирма—фирма";

- C2B (Consumer-to-Business) — "истемолчи—фирма";
- C2C (P2P — Peer-to-Peer, "тенг-тенг") "истемолчи-истемолчи";
- B2G ёки B2A (Business-to-Government, Business-to-Administration) — "фирма-давлат";
- G2B ёки A2B (Government-to-Business)—"давлат-фирма";
- G2C ёки A2C (Government-to-Consumer ёки Administration-to-Consumer) — "давлат-истемолчи";
- C2G ёки C2A (Consumer-to-Government) — "истемолчи-давлат";
- G2G ёки A2A (Government-to-Government) — "давлат-давлат";
- E2E (Exchange-to-Exchange) — "биржа-биржа";
- Интернет-банкинг;
- Интернет-трейдинг;
- Интернет-хизматлари: электрон тижорат занжирининг технологик хизмати: электрон тўлов, товарларни этказиб бериш, консалтинг хизматлари, илмий тадқиқот хизматлари ёки Интернет орқали суғурталаш.

B2B ёки бизнес-бизнес тизими. Ушбу тизим икки ташкилот ўртасида савдони амалга оширади. Ҳозирги кунда бизнес-бизнес тизими Интернет тармоғида кенг тарқалган электрон тижорат туридир. Ушбу тизимда амаллар Web-саҳифадан керакли товарларни танлаш ва онлайн тўловни амалга ошириш орқали амалга оширилади.

Бизнес-истемолчи ёки B2C тизими. Ушбу тизимда ташкилот юридик шахслар билан эмас балки тўғридан-тўғри истемолчи билан савдони амалга оширади. Ушбу тизимда истемолчи керакли товар ёки хизматни масофадан туриб, танлаши, унинг хусусиятлари ҳақида маълумотларга эга бўлиши, сотиб олиши ва тезкорлик билан уни олиб келтириши мумкин.



1-расм. Электрон тижорат модели

C2C ёки истемолчи-истемолчи тизими. Ушбу тизимда ҳеч бир ташкилот аралашмасдан икки жисмоний шахс ўртасида амалга оширилади. Бунинг яққол бир мисоли, ҳозирги кунда энг оммабоп бўлган Интернет-аукциондир. Ушбу тизимда истемолчи товарни магазинда қараганда арзонроқ нархда харид қилиши мумкин.

IOTP (Internet Open Trading Protocol) стандарти Интернет тармоғида очик электрон савдо протоколидир. Ушбу протокол тўлов тизимларини фойдаланишларини қамраб олиш мажбуриятига эга эмас. Ушбу стандарт қайтар жараёнга асосланган бўлиб, сотувчи ва истемолчи ўртасидаги шартнома, ҳисоб китоб, пул ўтказмаларини ўзида қамраб олади. IOTP қуйидагиларни қўллаб-қуватлайди:

- Савдонинг мавжуд моделлари
- Савдонинг янги моделлари
- Глобал мосликни.

Ушбу стандарт қуйидаги: MasterCard Credit, Visa Credit, Mondex Cash, Visa Cash, GeldKarte, eCash, CyberCoin, Millicent, Proton ва ҳ.к тўлов

турларини қўллаб қуватлайди. Ушбу стандарт тўловни ёки интернет магазин тизимини қандай дастурий воситалар асосида қуриш каби имкониятларни қўллаб қуватламайди, фақат электрон савдони амалга ошириш учун умумий қолипни аниқлаб беради.

ЮЭП нинг Интернет тармоғида қуйидаги турдаги амалларни бажаради[17,18]:

- Сотиб олиш. Бу хизмат, сотиб олиш, тўлов ва етказиб беришлардан иборат.
- Қайтариш. Олдин амалга оширилган харид тўловини қайтариш.
- Қиймат бўйича алмашиниш. Бу ўзида икки тўловни қамраб олади, масалан пул алмаштриш пайтида.
- Аутентификация. Ташкилот ёки шахсларни ҳақиқиёлигини текшириш.
- Тўлов тақризи. Молиявий тизимдан электрон тўлов тақризини амалга ошириш.
- Депозит. Молиявий тизимда қурилма депозитини амалга ошириш.
- Сўров. Бажарилаётган пайтда ёки бажарилиб бўлингандан сўнг ЮЭП амаллари ҳолати ҳақида сўровни амалга ошириш.
- Пинглаш. ЮЭП нинг бутун ҳолатини аниқлаш учун берилган оддий сўров.

ЮЭП, (Joint Electronic Payment Initiative) – сотиб олиш ва тўлаш орасидаги жойлашган[17].

ЮЭП стандарти қуйидаги уч турдаги протоколга асосланади:

1. SET (Secure Electronic Transactions) – стандарт протокол бўлиб, хавфсиз бўлмаган тармоқда банк ва кредит билан боғлиқ амалларни бажариш учун ишлаб чиқилган. SET тўлов тизими саналмай, пул ўтказмалари жараёнида аутентификациялаш учун хавфсизлик протоколларини ўзида мужассам этган. Бу эса фойдаланувчиларни очиқ тармоқдан хавфсиз фойдаланишларини таъминлайди. Ушбу протокол машҳурликка эришмагандан сўнг, VISA 3-D Secure XML протоколин

таклиф этди.

2. PEP (Protocol Extension Protocol) – Web-серверда HTML стандарти устида бажариладиган амаллар пратоколи.
3. UPP (Universal Payment Preamble) – сотувчилар учун ҳисоблаш методларини аниқлаш музокара пратоколи.

2. Электрон тўлов тизимлари

Интернет тармоғи орқали электрон тижоратни ривожланиши натижасида, сўнги 10 йилликда кўплаб тўлов турлари пайдо бўлди. Электрон тўловларни таснифлашда ва турларга ажратишда бир неча ёндошувлар мавжуд. Масалан, Murthy 6 та электрон тўлов турини ажратади: РС-Банкинг, Кредит карталар, Электрон чеклар, Микро тўлов, Смарт карта ва Электрон кашелок. Калакота ва Винстонлар эса 3 турдаги электрон тўлов турини ажратишади: электрон тўлов тизимларига асосланган рақамли токенлар, электрон тўлов тизимларига асосланган смарт карталар, электрон тўлов тизимларига асосланган кредитлар. Денис эса уларни икки: Электрон кашелок ва электроник дебит карталари тизими. Шулардан келиб чиқиб электрон тўлов турларини қуйидаги тўрт тоифага ажратиш мумкин[12]:

- Онлайн кредит карта тўлов тизими;
- Электрон чек тўлов тизими;
- Электрон пул тизими;
- Электрон тўлов тизимларига асосланган смарт карталар.

Онлайн кредит карта тўлов тизими . Ушбу турдаги тўлов турлари ҳозирда кенг тарқалган электрон тўлов тизими саналиб, харидор ва сотувчи орасида олди-сотди амалини янада осонлаштиради. Унинг афзалликлари қуйидагилар: шахсийлик, бутунлик, мослик, яхши транзакция амалга оширилиши, ҳаракатланиш имкони мавжудлиги, кичик даражадаги молиявий хавф ва анонимлик. Ушбу тоифадаги тўлов тури кенг фойдаланилишига қарамасдан, бир қанча камчиликларга эга. Булар аутентификация масалалари билан боғлиқ бўлса, бошқа томондан эса ушбу картани қалбакилаштириш

имкони мавжудлиги ва ушбу тоифадаги хавфларни ҳозирда кенг тарқалганлиги.

Ушбу турдаги онлайн тўлов тури жуда содда бўлиб, истемолчи Интернет магазиндан ўзига керакли товар ёки хизматни танлайди ва кредит карта ҳақидаги ва мижоз маълумотларини киритади. Натижада, юборилган маълумотлар авторизациядан ўтказилади[12].

2-расм. Онлайн карта ёрдамида тўлаш

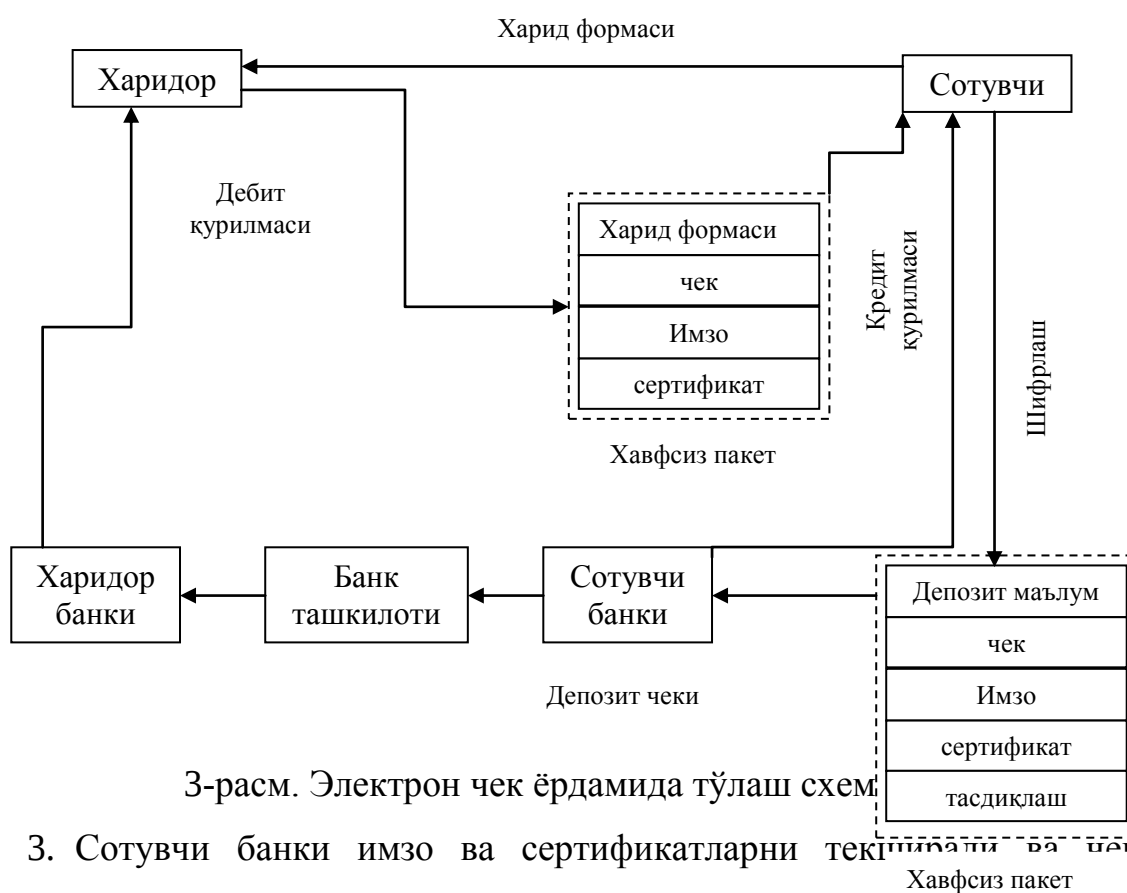
Ушбу турдаги тўлов турлари қуйидаги 3 категорияга асосланади:

- Фақат кредит карта маълумотлари асосида аутентификациядан ўтиш;
- Шифрланган кредит карта маълумотлари асосида аутентификациядан ўтиш;
- Учинчи томон асосида аутентификациядан ўтиш.

Электрон чек тўлов тизими. Ушбу турдаги тўловда ананавий чекка ўхшаш, фақат электрон ҳужжатга электрон имзо қўйиш орқали амалга ошириладиган тўлов турига айтилади. Бу тўлов тури бир қанча қулайликларга эга: сотувчига харидор томонидан маълумотлар тақдим этилиши шарт эмас, мижоз ҳақидаги маълумотларни Web-саҳифа орқали жўнатиш мажбурияти йўқлиги, ананавий тўловга қараганда пул ўтиш тезлигининг катталиги ва ҳ.к. Ушбу турдаги тўлов асосан ташкилотлар орасида ёки давлатлар орасида пул алмашинишида кенг қўлланилади.

Ташкилот ва харидор ўртасида фойдаланиш унчалик қулай эмас. Электрон чек орқали тўловни амалга ошириш қуйидаги тартибда амалга оширилади:

1. Харидор харид формасини тўлдиради, электрон чекни қўшади, махфий калити билан имзо қўяди, очик калитни қўшади, махфий калит билан шифрлаб, сотувчига жўнатади.
2. Сотувчи махфий калитидан фойдаланган ҳолда маълумотни дешифрлайди, харидор сертификатини, имзосини ва чекни текширади. Ўзининг депозит маълумоти ва очик сертификатини қўшиб шифрланган ҳолда ўзининг банкига жўнатади.



3-расм. Электрон чек ёрдамида тўлаш схем

3. Сотувчи банки имзо ва сертификатларни текшириб, баъзи транзакцияни ўтказиш марказига жўнатади. Ушбу икки ташкилот бир-бири билан хавфсиз канал орқали боғланган.
4. Транзакция амалга оширилгандан сўнг, сотувчи баланси ўзгаради ва кредит қурилмасига хабар жўнатилади.
5. Харидорга бўлган транзакция ҳақида маълумот этказилади.

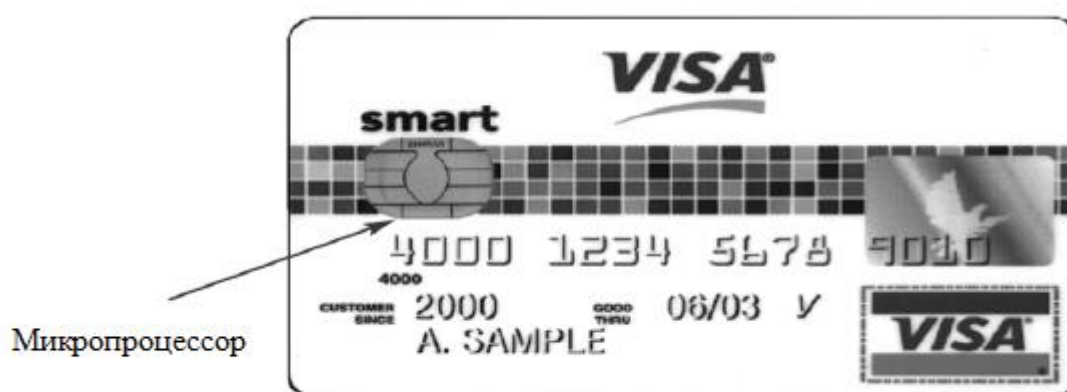
Электрон чеклар Интернет тармоғида хавфсиз тўлов тизимини яратиб, кейинчалик ҳам кам харажат билан фойдаланишда қўл келади.

Электрон пул тизими. Ушбу тўлов тизими онлайн тўлов тизимлари орасида янгиларидан саналиб, ананавий қоғоз пул билан тўлашни электрон кўринишда хавфсиз ва шахсийлаштирилган шаклидир. Ушбу рақамли пул орқали тўлов тизими авторизациялашда қулайлик, шахсийлик, кам транзакция қийматли каби бир қанча қулайликларга эга бўлсада, кам тарқалганлиги, юқори молиявий таҳдид мавжудлиги каби заифликларга эга[12].

Валюта тури	Қиймати	Авторизация маълумоти	Рақамли имзо	Нусхалашдан ҳимоя воситаси
-------------	---------	-----------------------	--------------	----------------------------

4-расм. Электрон пул тузулиши

Электрон тўлов тизимларига асосланган смарт карталар. Смарт карталар онлайн тўлов тизими тури сифатида уни қайтадан ташкил этди. Ушбу қурилма ҳам кредит карта ҳажмига тенг ҳажмда бўлиб, унда ҳам махсус микропроцессор мавжуд. Ушбу микропроцессор кредит картадагига нисбатан каттароқ маълумот ҳажмига эга.



5-расм. Смарт карта

Ушбу смарт карталар Осиё ва Европа мамалакатларига кенг тарқалган. Ушбу тўлов тури орқали кенг ҳажмда тўловни амалга ошириш мумкин. Масалан, солиқ тўловларини амалга оширишда, телефон карта каби, дебит карта маълумотларини сақлаш учун ва ҳ.к. Ананавий электрон пул тизимлари билан солиштирганда, смарт карталарга асосланган тўлов тизимлари жорий вақтдаги маълумотларни талаб этмайди.

Ушбу электрон тўлов турларидан ҳар хил давлатда ҳар хил фойдаланилади. Қайси электрон тўлов турини кўпроқ фойдаланилиши давлатнинг молиявий тизимидан келиб чиқади. 2003 йилда дунё бўйича бўлган барча электрон тўловларни 94.1 % кредит карталарга тўғри келади. Бу кўрсаткич ҳозирда ҳам ўз мавқеини йўқотмаган [12].

1-жадвал

Электрон тўлов турлари таҳлили

Хусусият	Онлайн кредит карта	Электрон пул	Электрон чек	Смарт карта
Тўлов вақти харақати бўйича	Кейин тўланади	Олдиндан тўлов	Кейин тўланади	Олдиндан тўлов
Транзакция маълумотларини узатиш	Магазин ва банк кредит карта ҳолатини текширади	Ихтиёрий. Томонлар исмларини қолдиришга ҳожат йўқ.	Электрон чек ёки кўлов кўрсаткичи тасдиқланиши шарт	Икки томондаги смарт карталар трансферини амалга оширади
Онлайн ва офлайн транзакция	Онлайн транзакция	Онлайн транзакция	Офлайн транзакцияга рухсат берилган	Офлайн транзакцияга рухсат берилган
Банк ҳисоби жараёни	Кредит карта ҳисоби орқали	Йўқ	Банк ҳисоби орқали	Смарт карта орқали
Фойдаланувчилар	Бирон бир қонуний кредит карта эгаси	Бирор бир шахс	Банк ҳисоби мавжуд бўлган бирор бир шахс	Банк ёки кредит карта ҳисобига эга бўлган бирор бир шахс
Тўловни ёзиб борадиган томон	Таксимланган банк	Савдо шаҳабчаси	Савдо шаҳабчаси	Савдо шаҳабчаси
Истемолчи транзакциясида хавф	Кўплаб хавфлар банк томонидан ҳимояланади	Истемолчи электрон пулни ёқотиб қўйиши хафи	Истемолчига кўплаб хавфлар мавжуд, лекин истемолчи ихтиёрий вақт ҳисобни тўхтатиши мумкин	Смарт карта йўқолиши ёки фойдаланиб бўлмаётганини қилиши
Ҳозирги вақтдаги оммабоплик даражаси	Халқаро ва кенг тарқалган тўлов тури	Бир бирига мос молиявий стандартлар орасида тарқалган	Оммабоп эмас	Халқаро ва ҳозирда кенг тарқалаётган тўлов тури
Анонимлик	Қизиқишга ёки тўлиқ аноним	Тўлиқ аноним	Анонимлик йўқ	Тўлиқ аноним, зарур бўлганда марказий банк сўраш ҳуқуқига эга

Кичик тўловлар	Транзакция қиймати баланд. Кичик тўловларга мос эмас.	Транзакция қиймати паст. Кичик тўловлар учун.	Лимитгача фойдаланилади. Кичик тўловлар учун қулай.	Транзакция қиймати паст. Лимитгача фойдаланилади. Кичик тўловлар учун мос.
Маълумотлар базасида(МБ) сақланган маълумотлар	Кредит карта ҳисоби маълумотлари доимий сақланиши шарт.	Электрон тўловда фойдаланилган серия рақамини сақлаш учун катта ҳажмдаги МБ	Доимий ҳисоб маълумотлари сақланади.	Доимий ҳисоб маълумотлари сақланади.
Транзакция маълумотлари номинал қиймати	Имзоланади ва лимит билан эркин чиқарилади	Номинал қиймат ўрнатилади ва ўзгармайди.	Имзоланади ва лимит билан эркин чиқарилади.	Лимитга мос эркин айрилиши мумкин.
Реал/вертуал дунё	Реал дунёда фойдаланилиши мумкин.	Фақат вертуал фойдаланилиши мумкин.	Вертуал дунёда чекланган, аммо реал дунёда кенг тарқалган.	Реал ёки вертуал дунёда фойдаланилиши мумкин.
Трансфердаги чегара	Кредит карта лимитига боғлиқ	Қанча тўланишига боғлиқ	Чегара йўқ.	Қанча пул сақланишига боғлиқ.
Ҳаракатла нувчанлик хоссаси	Бор	Йўқ	Йўқ	Ҳа

3. Ананавий тижорат тўлов тизимларида хавфсизлик

Интернет тўлов тизими-Интернет тармоғида олди-сотдини амалга ошириш учун Интернет-фойдаланувчилари, бизнес-ташкилотлар ва молиявий ташкилотлар ўртасида тузулган тизим.

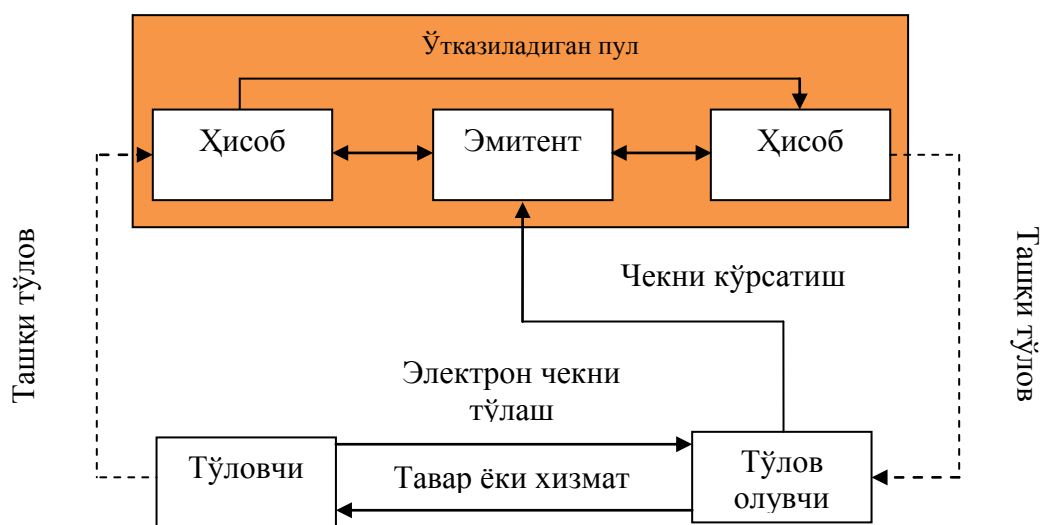
Электрон тижоратда тўлов тизимлари қуйидаги талабларга риоя қилган ҳолда амалга оширилиши керак:

- Конфиденциалликка риоя қилиш. Интернет тармоғи орқали тўловни амалга ошириш жараёнида маълумот фақат харидор ва сотувчи ташкилот учун мавжуд бўлиши, бошқалар учун махфий бўлиши.
- Ахборот тўлиқлигини сақлаш. Тўлов ҳақидаги ахборотни ҳеч ким ўзгартирмаслиги керак.

- Аутентификация. Сотувчи ва харидор бир бирларини ҳақиқийлигларини билишлари шарт.
- Тўлов жихозлари. Тўлов жихозларидан мавжуд фойдаланувчиларни ихтиёрий вақтда фойдаланиши.
- Авторизация. Ушбу жараён транзакция вақтида талабга кўра тўлов тизимини амалга ошириш икони мавжудлиги ёки мавжуд эмаслигини билдиради. Ушбу жараён сотиб олувчидан нақд суммани мавжудлигини талаб этади.
- Сотувчи таваккалига кафолат. Интернет тармоғида сотувчи, товарни бекор қилиш ёки виждонсиз харидорлар билан боғлиқ кўплаб таваккалчиликка дучор бўлади. Ушбу таваккалчиликларни ҳал қилиш тўлов тизими правайдерлари ва бошқа ташкилотлар билан боғлиқ равишда амалга оширилиши шарт.

Юқорида айтиб ўтилган барча талаблар Интернет тармоғида мавжуд барча тўлов тизимларида мавжуд бўлиши шарт. Барча тўлов тизимлари тўлов шакли бўйича қуйидаги турларга бўлинади[17,18,19]:

- Дебет(электрон чек ва рақамли нақд пул билан ишловчи);
- Кредит (кредит карта билан ишловчи).



6-расм. Тўлов ўтказиш шакли

Дебет тизими. Дебет тизими ананавий тўлов тизимидаги оддий чекка ва пулга ўхшаш электрон чек ва электрон пул асосида амалга оширилади. Ушбу тизимда икки томон: эмитентлар ва фойдаланувчилар. Эмитент бу тўлов тизимини бошқарувчи субъект. У электрон чекларни ҳосил қилади. Фойдаланувчи эса ҳосил қилинган электрон пул ёки чеклар ёрдамида Интернет тармоғидан тўловларни қабул қилади ва амалга оширилади.

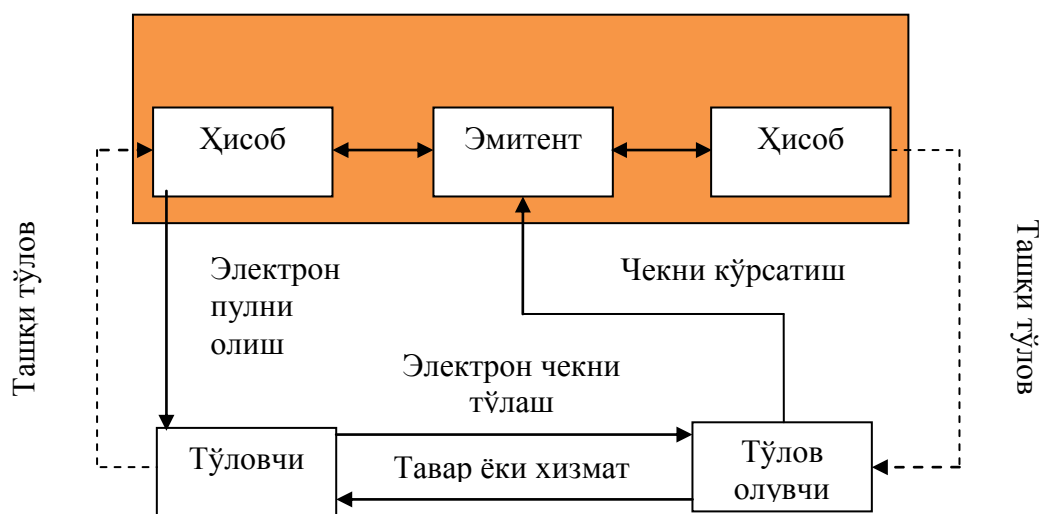
Электрон чек оддий ананавий чек каби бўлиб, унда оддий имзо эмас электрон имзо қўйилади. Бу амаллар одатда банклар томонидан амалга оширилади.

Электрон пул оддий пул қийматига эга саналган электрон кўринишдаги қиймат. Электрон пулдан фойдаланишнинг асосий мақсад Интернет тармоғида сотувчи ва харидор ўртасидаги олди-сотди амалини осонлаштириш.

Дастлаб банкда ҳақиқий пул электрон кўринишда ўтказилади. Ушбу кўринишни сақлаш турида қараб икки турга бўлинади:

- Компьютернинг қаттиқ дискида сақланувчи;
- Смарт карталарда сақланувчи.

Қуйида электрон пул асосида тўловни амалга ошириш схемаси келтирилган:



7-расм. Электрон пул билан тўлов тизими

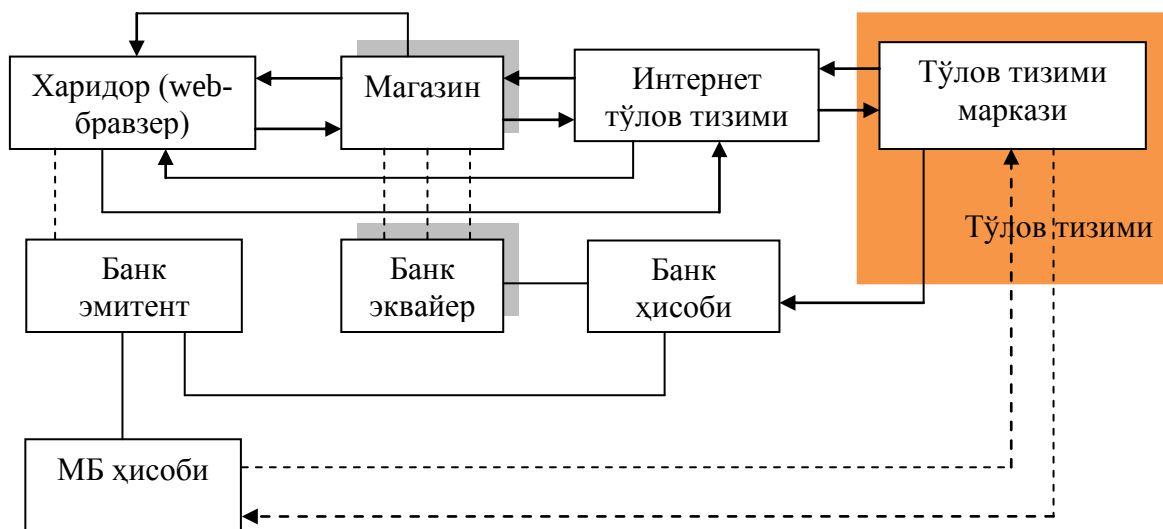
Ананавий тўлов тизимларида хавфсизлик қуйидаги қуйидаги параметрлар орқали амалга оширилади:

- Ҳар бир пластик карточка учун махфий саналган PIN код орқали;
- Фойдаланилаётган пайтда истесолчи ҳақиқийлигини тасдиқлаш орқали.

Анавий тўлов усулида бевосита истемолчининг ўзи қатнашганлиги сабабли хавфсизлик масаласи долзарб саналмайди. Фақат фойдаланувчи картаси ўғирланиш, ёқотилиш ёки нусхалаш амалларидан сақланса ҳамда фойдаланувчи пароли (PIN коди) махфий тутилса бўлди.

4. Электрон тижорат хавфсизлиги

Кредит карточкадан фойдаланган ҳолда интернет орқали тўлаш тизими Интернетда кредит карточка билан тўлаш тизими одатий тизимдаги, кредит карта билан тўлаш кабидир. Барча транзакциялар Интернет орқали бўлганлиги сабабли, фарқли равишда хавфсизлик масаласи ва аутентификация масаласи қўшилади[17,18].



8-расм. Кредит карта ёрдамида тўлов тизими

Юқорида келтирилган Интернетда кредит карточка орқали тўлаш схемасида қуйидаги ташкил этувчилар мавжуд:

1. Харидор. Компьютер билан Интернет тармоғида савдони амалга оширувчи мижоз.
2. Банк эмитент. Бу ерда харидор ҳисоб рақами жойлашган. Банк эмитент фойдаланувчилар кафолатли молиявий амалларни амалга

оширишлари учун катралар беради.

3. Сотувчи. Ушбу сервер харидорлар учун керакли бўлган товарлар билан бойитилган вертуал магазин.
4. Банк-эквайер. Сотувчига хизмат қилувчи банк. Ҳар бир сотувчи бирон бир банкда ўзининг ҳисоб рақами мавжуд бўлади.
5. Интернет тўлов тизими. Ҳар бир ташкил этувчилар (сотувчи, харидор, банк эмитент ва ҳ.к) ўртасида улаб берувчи вазифасини бажаради.
6. Ананавий тўлов тизими. Берилган кредит картага хизмат кўрсатувчи техник ва молиявий жихозларнинг комплекси. Асосий бажарадиган иши харидор ва сотувчи орасидаги ҳисоб китоб ишларини амалга ошириш.
7. Тўлов тизими маркази. Ананавий тўлов тизимлари орасидаги технологик ва ахборот алмашинувларни амалга оширувчи ташкилот.
8. Тўлов тизимларининг ҳисоб банки. Тўлов тизими марказидан олинган ахборот асосида томонлар ўртасида ҳисоб-китобни амалга оширувчи кредит ташкилоти.

Юқоридаги тузилма қуйидаги тартибда ишлайди:

1. Харидор интернет магазин орқали ўзига керакли товарни танлайди, уни корзинкага қўшади ва кредит карта билан тўлаш усулини танлайди.
 2. Шундан сўнг, карта ҳақидаги барча маълумотлар (рақам, карта эгаси исми, ҳаракатни тугаш вақти) Интернет тўлов тизими марказига авторизация учун юборилади. Ушбу амаллар икки усудда амалда амалга оширилиши мумкин:
 - Маълумотлар вертуал магазин орқали Интернет тўлов тизими марказига юборилиши мумкин;
 - Тўғридан-тўғри Интернет тўлов марказига юборилиши мумкин.
- Кўриниб тургани каби кўп ҳолларда иккинчи усуддан фойдаланилади. Бу усудда харидор кредит картаси маълумотлари

вертуал магазинда ушлаб қолинмайди ва сақланмайди. Бу эса магазин орқали бузгунчининг харидор маълумотларини олишни тақиқлайди.

Ушбу ҳолатда маълумот алмашилиш жараёнида хавфсизликни таъминлаш каналларни шифрлаш орқали амалга оширилади. Бунинг учун кўп ҳолларда SSL(Secure Sockets Layer) пратоколидан ёки SET пратоколларидан фойдаланилади.

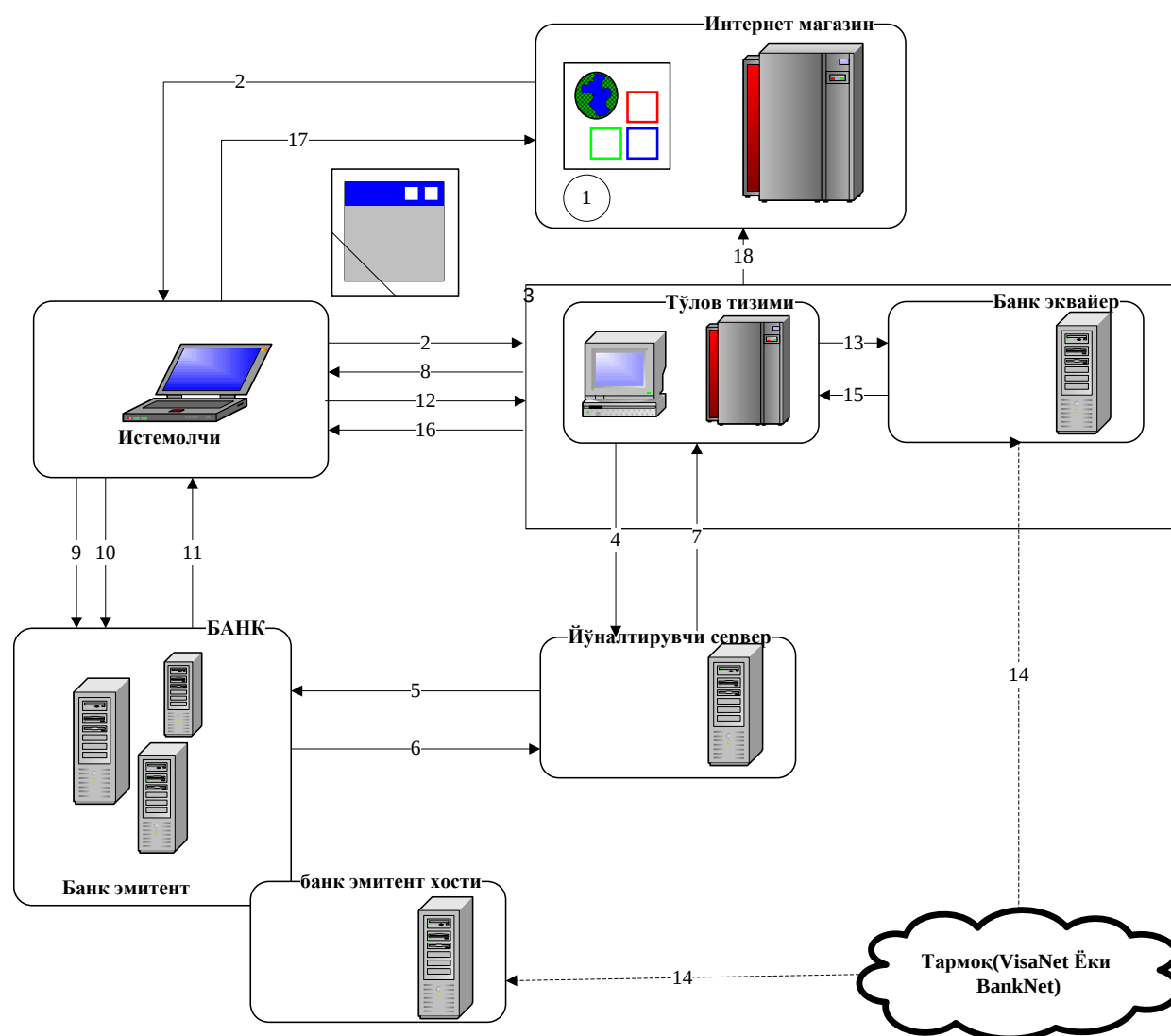
3. Интернет тўлов тизими маркази олинган сўровларни тасдиқлаш учун ананавий тўлов тизими марказига юборади.
4. Тўлов тизими маркази сўровларни тасдиқлаш учун маълумотлар базасига(МБ) жўнатади. Маълумотлар маркази банк-эмитентга сўров юбориб картани авторизациядан ўтказди.
5. Олинган натижа Интернет тўлов марказига юборилади.
6. Магазин авторизация маълумотларини олади.
7. Харидор ҳам магазин ёки Интернет магазин орқали авторизация маълумотларини олади.
8. Авторизация муофакиятли амалга оширилганда
 - Магазин товар ёки хизматни фойдаланувчига кўрсатади;
 - Тўлов тизими маркази эса авторизация маълумотларини банк ҳисобига юборади. Банк ҳисоби эса банк-эмитент ва банк-эквайер ёрдамида ҳисоб китобни амалга оширади.

CNP-транзакцияда (Cardholder Not Present) электрон тўлов тизимида тўловни амалга оширишда пластик картадан фойдаланиш тизимини кўрсатди. Ушбу тизим савдо марказларида фойдаланувчи ўзи қатнашмасдан, пластик картадан фойдаланган ҳолда авторизациядан ўтиши асосида яратилган[17,18,19].

Ушбу жараён қуйидагича амалга оширилади. Истемолчи компьютер ёрдамида Интернет магазиндан ўзига керакли товар ёки хизмат турини танлайди. Шундан сўнг унинг хусусиятлари билан танишиб, уни сотиб олиш учун ўзининг пластик картасидан фойдаланишни белгилайди(1.9-расм).

Кейин эса истемолчи ва сотувчи ўртасида бир-бирларини ҳақиқийдигини билиш учун аутентификация жараёни амалга оширилади. Бунда мижоз томонидан пластик карта реквизитлари фойдаланилади.

Олинган мижоз маълумотлари савдо ташкилоти банкига юборилади ва бу ерда авторизация хабари шакллантирилади. Ушбу авторизация хабари банк-эмитентга юборилади ва ундан авторизациядан ўтади. Бунинг натижаси эса ташкилот хизмат банкига ва пластик карта эгасига юборилади. Шундан сўнг мижоз электрон кўринишдаги чекни олади.



9-расм. Пластик карта орқали сотиб олиш тизими

Электрон тижоратда хавфсизликни таъминлашда шуни этиборга олиш керакки, оддий транзакцияда фойдаланилган аутентификация усуллари этарли эмас.

Оддий транзакцияларда ананавий магазинда тўловни амалга оширишда сотувчи харидорни ҳақиқийлиги тасдиқлаш учун ундан бирон бир ҳужжат талаб этади.

Электрон тижоратда эса бузғунчи учун пластик карта реквезитларини билишни ўзи кифоя қилади. Бу ҳолда ҳеч қандай сохта пластик карта ёки сарф –харажатлар ҳақида маълумот керак бўлмайди.

Пластик карталар оламида магнит паласалари муҳим аҳамиятга эга. Масалан, оддий тўлов тизмини амалга оширишда пластик карта ва унинг махфий калити, PIN –коди зарур бўлади. PIN –код ҳам ўз ўрнида 4-12 хонали махфий, фақат мижозга тегишли бўлган маълумот. Электрон тижоратда эса ушбу PIN-кодни ўзини билиш кифоя. Пластик карта бўлиши эса талаб этилмайди. Бу эса фақат PIN –код мижоз ҳисобини хавфсизлигини таъминлайди эмас ва бунинг учун этарли саналмайди.

Ушбу ҳолатни олдини олиш учун эса транзакция давомида юбориладиган маълумотлар шифрланган кўринишда акс эттирилиши шарт. Бу махфий маълумот эса фақат мижоз ва банк-эмитентга маълум бўлиши керак. Ҳозирги кунда ушбу муаммони ҳал қилишда PIN-PAD деб номланувчи махсус аппарат-дастурий қурилмадан фойдаланилади. Ушбу қурилма транзакция маълумотларини ишончли сақлайди. Мижоз ўз PIN-кодини киритиш билан қурилма орқали у шифрланган кўринишда келтирилади ва Интернет тўлов тизими орқали мижоз банк-эмитент тизими билан боғланади. Олинган шифрланган маълумот банк-эмитентда мавжуд калит билан дешифрланади ва авторизациядан ўтказилади. Ҳар бир шифрлаш калитлари банк-эмитенти тизимида сақланиши эса тизимда хавфсизлик даражасини янада оширади.

Бундан ташқари ананавий усулни, қуйидаги тартибда ривожлантириш мумкин. Банк-эмитент билан мижоз ўртасида маълумотларни шифрлаш учун ассиметрик тизим калитлари тақсимланади. Масалан, мижоз банк-эмитентдан ўзининг очиқ калитни олади. Транзакция маълумотларини айнан шу очиқ калит билан шифрлайди. Банк-эмитент эса шифрланган

маълумотларни ўзида мавжуд махфий калит билан дешифрлайди. Олинган маълумот асосида авторизация амалга оширилади.

Классик саналмаган қуйидаги усулда эса, мижоз калитни юборишдан ташқари, унга қўшимча равишда транзакция маълумотларини (мижоз ва банк-эмитентга маълум бўлган) юборади. Бу эса авторизациядан ўтиш жараёнида ишончлилиқ даражасини оширади. Бу усулда калитларни узатиш муаммоси юзага чиқиб, ушбу муаммо ҳал қилинса катта натижага эришилиш мумкин.

STB CARD дан фойдаланган ҳолда хавфсизлиқни таъминлашда эса, ушбу пластик карта хотирасида банк-эмитент томонидан қўшимча PIN-2 коди қўшилади. Ушбу 16 узунликдаги фақат мижоз ва банк-эмитентга тегишли бўлиб, PIN-конвертни очишда фойдаланилади. PIN-конверт эса махфий калит, карта рақами ва бошқа махфий маълумотлардан иборат бўлади. PIN-2 калит эса транзакция маълумотларини ва PIN-конвертни ҳосил қилишда ва очишда симметрик шифрлаш калити ўрнида фойдаланилади. Ушбу усул қуйидаги камчиликларга эга:

- PIN –кодни текшириш учун, Интернет магазин java-апплетидан фойдаланган бўлиши керак. Ушбу технология тизим ҳажмини камайтиради.
- 16 та ўн олтилик санок тизимидаги рақамларни пластик картадан фойдаланиш ноқулайлиги;
- Бузғунчи PIN-2 кодни билган тақдирда мижоз ўрнидан туриб барча ишларни амалга ошириш имкониятини қўлга киритади.

Ушбу олинган таҳлил натижаларидан келиб чиқиб шуни айтиш мумкинки, ахборот хавфсизлиги даражаси муҳим аҳамиятга эга.

Шуни ҳисобга олиб хавфсизлиқ қуйидаги ташкил этувчиларни талаб этади:

Олди-сотди жараёнида қатнашган қатнашувчиларни аутентификациялаш. Бунда истемолчи пластик картаси реквезитлари

интернет магазин ва сотувчи банк тизими учун ҳақиқий бўлиши шарт. Ўз ўрнида mijoz ҳам тўлов қабул қилувчи банкни ҳақиқийлигини билиш шарт.

SSL – mijoz ва сервер ўртасида хавфсиз алоқани ўрнатиш учун ишлаб чиқилган криптографик пратокaл. Ушбу пратокaл орқали эса HTTPS пратокaли ишлаб чиқилди. Ушбу пратокaл Netscape Communications компанияси томонидан ишлаб чиқилган. Охирги ишлаб чиқилган варианти SSL 3.0 саналиб, унга TLS номи берилди.

Ушбу пратокaл сервер ва mijoz ўртасида маълумотлар алмашинувида конфиденциялликни таъминлайди. Бунинг учун ассиметрик шифрлаш алгоритмларидан фойдаланади.

2-жадвал

HTTPS пратокaли таҳлили

Пратокaл версияси	Хавфсизлиги	Сайтларни қўллаб-қуватлаши
SSL 2.0	Йўқ	28.4 %
SSL 3.0	Бўлиши мумкин	99.8 %
TLS 1.0		99.4 %
TLS 1.1	Бор	10.4 %
TLS 1.2		12.7 %

Ушбу пратокaл ўзида қуйидаги уч хусусиятни жам қилган:

- Аутентификациялаш. Белгиланган алгоритм бўйича сервер ва mijoz ўртасида аутентификацияни амалга оширади.
- Тўлиқлик. Маълумотларни алмашилиш жараёнида маълумотни тўлалигини таъминлайди.
- Шифрланган канал. Уланиш ўрнатилгандан сўнг барча трафикни шифрлаш.

Ушбу пратокaлда қуйидаги криптографик алгоритмлардан фойдаланилади:

- Калит алмашилишда ва маълумотларни тўғрилигини ҳисоблашда: *RSA, Diffie-Hellman, ECDH, SRP, PSK*;
- Аутентификациялашда: *RSA, DSA, ECDSA*;

- Симметрик шифрлаш учун: *RC2, RC4, IDEA, DES, Triple DES, AES, Camellia*;
- Хэш функция: *SHA, MD5, MD4, MD2*.

5. Ўзбекистонда мавжуд электрон тўлов тизимлари

Ҳозирда Ўзбекистонда Интернет-магазин савдо тизими ва электрон тўлов тизимлари жадаллик билан ривожланмоқда. Шулардан қуйидаги электрон тўлов тизимлари кенг тарқалган:

1. Paynet;
2. WEBSUM;
3. SMS to'lov;
4. Click.

WEBSUM. WEBSUM электрон Интернет тўлов тизими бўлиб, аппарат-дастурий воситалар мажмуидан ташкил топган. Ушбу тўлов тизимида барча амаллар “сўм” ҳисобида амалга оширилади.

WEBSUM тўлов тизими Ўзбекистон Республикаси ҳудуди бўйлаб тарқалган ва UzCard Visa Sum кредит карталари орқали тўловни амалга оширади.

WEBSUM тўлов тизимининг вазифалари қуйидагилар:

- Ўзбекистон ҳудудида электрон тижорат соҳасида ишончли тўлов тизимини яратиш;
- Ўзбекистон ҳудуди бўйлаб онлайн тўловни амалга оширишда кенг фойдаланиш;
- Интернет тармоғи орқали фойдаланувчига қулай тўлов тизимини тақдим этиш;

Ушбу тўлов тизими орқали қуйидаги тўловларни амалга ошириш мумкин:

- Мобиль операторларига тўловни амалга ошириш;
- Интернет провайдерлари учун тўлов;
- Skype, TorgUz;

- www.odnoklassniki.ru, ВКонтакте ижтимоий тармоқларида;
- машҳур онлайн ўйинлар учун;
- рақамли телевидения;
- домен ва хостинг сотиб олишда;
- Интернет магазинда тўловни амалга оширишда;
- Темир йўл ва авиа билетларини сотиб олишда;
- Меҳмохоналарда;
- Коммунал тўловларни амалга оширишда.

Ушбу тўлов тизимидан фойдаланиш учун фойдаланувчи рўйхатдан ўтади ва ID олади. Олинган ID ҳисобини тўлдириш учун эса банкомат орқали UzCard билан, банк шахобчаларидан, интернет-банкнинг SAM.online ва халқаро тўлов тизимлари орқали амалга ошириш мумкин.

SMS to'lov. SMS-To'lov» нақд пулсиз тўловлар тизими – бу мижозлар ва компания ўртасидаги, мижозлар банк ҳисобларидан электрон тўловни амалга оширувчи банк автоматлаштирилган тўловларларни бошқариш тизими билан бирлаштирилган тўловлар процессинг тизими [21].

«SMS-To'lov» тизимининг устунликларини яққол кўриш мумкин. Ушбу тизим Шахсий кабинет орқали ёки Мобиль илова орқали СМС- хабарлар жўнатиш ёрдамида нақд пулсиз тўловларни амалга ошириш имконини тақдим этади. «SMS-To'lov» тизими фойдаланувчилари учун тўловлар қабул қилиш пунктларини излаш зарурати йўқ. Барча тўловлар СМС ёрдамида амалга оширилади, осон, қулай, қийинчиликлар юзага келтирмайди. «SMS-To'lov» бир неча сонияда тўловни амалга ошириш имконини беради, бу еса яна вақтни максимал тежашни назарда тутди. Фойдаланувчилар банк шахсий ҳисобларида мавжуд бўлган пул маблағларидан максимал фойдаланадилар. Ва ниҳоят, «SMS-To'lov» - кун давомида 24 соат, ҳафтасига 7 кунда кафолатли тўловлардир.

Тизим «Ўзбекистон Миллий Банки», «Ҳамкорбанк», «АКБ Микрокредитбанк», «Асака» Банки, «Универсалбанк» ва «Инфинбанк» каби бир неча тижорат банклари билан шартномалар имзолаган.

«SMS-To'lov» тизимидан фойдаланганда мобилъ алоқа, интернет, солиқлар, суғурта, электрон савдоларда иштирок етиш (биржа шартномаларини, интернет-магазинлар тўловини амалга ошириш ва шу кабилар) каби хизматлар учун ҳақ тўлашни амалга ошириш имкониятлари пайдо бўлади, бундан ташқари коммунал хизматлар, шаҳар телефони учун ҳақ тўлаш, рақамли телевидение учун ҳақ тўлаш, авиа- ва темир йўл билетларини банд қилиш ва ҳақ тўлаш; меҳмонхона хизматлари ва ниҳоят барча сервис хизматларига ҳақ тўлаш тизимини татбиқ етиш режалаштирилмоқда. Шу билан бирга чакана савдони ҳам қамраб олишни режалаштирилмоқда. «SMS-To'lov» тизими ўз истемолчиларини охир-оқибат нақд пул еҳтиёжидан халос қилади.

«SMS-To'lov» тизими хизматидан фойдаланиб, банк пластик картангиз пул маблағларидан максимал фойдаланиш имкони бўлади.

«SMS-To'lov» тизими орқали ўз мобилъ телефонингизга ҳамда кўплаб турдаги товар ва хизматларга онлайн тўлов амалга оширишингиз мумкин. Бунинг учун сиз бир марта тижорат банкига ташриф буюришингиз керак бўлади («Ўзбекистон Миллий Банки», «Ҳамкорбанк», «Асака» банк, «Универсалбанк», «Инфинбанк» «АКБ Микрокредитбанк»). Бу ерда паспорт, ўз мобилъ телефонингизни тақдим етишингиз керак. Банк ходими бир неча дақиқа давомида «SMS-To'lov» тизимида сизни рўйхатга киритади, сизнинг мобилъ телефонингизга Java иловасини юклайди ва алоҳида логин ва парол тақдим этади, уларни сиз каттиқ сир сақлашингиз керак бўлади. Бу сизнинг мобилъ телефонингиз банк пластик карточкаси ҳисоб рақамига уланганлигини англатади. Ушбу банк пластик карточкаси бўлмаган тақдирда сизга ҳисоб рақами очилади, уни сиз нақд пул билан ҳамда истаган бошқа банк пластик карточкаси орқали тўлдириб боришингиз мумкин бўлади.

www.smst.uz сайтида сиз 5 та ўзингиз ёқтирган рақамларни танлашингиз мумкин, уларни кейинчали тўлдириб боришингиз ҳамда шахсий кабинетда ўз тўловларингизни (транзакцияларни) кўздан кечиришингиз мумкин. Мобилъ илова ёрдамида Интернет ресурслардан фойдаланмасдан

бир неча сония ичида турли хил товарлар ва хизматлар учун тўловларни амалга оширишингиз мумкин:

- Мобиль компаниялар хизмати.
- Коммунал хизматлар.
- Интернет провайдерлар хизматлари.
- Савдо-саноат палатаси хизматлари.
- Тизимда тўлов учун тест синовлари ўтказиладиган хизматлар ва товарлар:
- Шаҳар жамоат транспорти.
- Шаҳар телефон алоқаси.
- Солиқлар.
- Суғурта.
- Авиа ва темир йўл билетларини банд қилиш ва тўлаш.
- Меҳмонхона хизматлари.
- Такси хизматлари.

Paynet. Республикамизда UzPaynet компанияси 2005 йилда ўз фаолиятини бошлаган. “Paynet” тизими орқали илк бор тўловлар 2006 йилда амалга оширилган. Ҳозирда юртимизнинг барча жабҳаларида компаниянинг 25 000 дан ортиқ тўловларни қабул қилиш шохобчалари мавжуд. Ҳар куни Paynet шохобчаларида 2 млн. нафардан ортиқ киши тўловларни амалга оширади. Бугунги кунда UzPaynet компанияси 90 дан ортиқ хизмат етказиб берувчилар билан ҳамкорлик қилади.

- “Paynet” тизими ўз олдида мижозларга хизмат кўрсатишнинг янги ва сифатли даражасини таъминлаш ҳамда тўловларни қабул қилишнинг анъанавий усулларида қочиш, провайдерлик хизматларини кўрсатувчи операторлар ва уларнинг мижозлари учун тўловларни қабул қилишда максимал қулайликлар яратиш, шунингдек, замонавий технологиялар ва юқори сифатли хизматларга асосланган ҳолда аҳоли ва ташкилотларга хизматларнинг бошқа турларини ҳам тақдим этиш каби мақсадларни қўйган. Бунинг натижасида, “Paynet” тизими

провайдерлик хизматларини кўрсатувчи компания офисига бормасдан, уяли алоқа, Интернет, шаҳар телефони, коммунал хизматлар ҳамда реал вақт режимида ишловчи бошқа хизматларни тўлаш имконини беради.

CLICK. Ушбу тизим мобиль операторларидан фойдаланган ҳолда USSD/SMS сўровлар орқали электрон тўловни амалга оширишга асосланади. Бу тизим орқали супермаркет, ресторанларда, кинотеатрларда коммунал тўловларни амалга оширишда, мобиль тўловларни амалга оширишда ва ҳ.к фойдаланиш мумкин [20].

Тизим тўловни амалга оширишда икки усулдан фойдаланади:

- Интернет сайтда (<https://my.click.uz> , <https://m.click.uz>) керакли товар ва хизмат учун онлайн тарзда тўловни амалга ошириш;
- USSD сўрови (*880#) орқали мобиль телефондан фойдаланган ҳолда ихтиёрий вақтда фойдаланиш мумкин.

Тизим қуйидаги имкониятларга эга:

- Нақд пулсиз савдони амалга ошириш жойларида мобиль телефон орқали ва интернет тармоғидан фойдаланган ҳолда амалга ошириш имконияти;
- Тизим ичида фойдаланувчилар орасида пул ўтказмалари;
- Тўлов маълумотларини олиш;
- Ҳисобни текширишнинг онлайн тизими;
- Жараёнлар ҳақида SMS жавоб олиш;
- Кўплаб соҳаларда тўловни амалга ошириш.

I боб бўйича хулосалар

1. Ананавий тижорат ва электрон тижорат, электрон тижоратнинг афзалликлари ҳақида тўхталди;
2. Электрон тижорат моделлари билан танишиб чиқилди ва B2B ёки B2C (бизнес-бизнес, бизнес-истемолчи) тизими танлаб олинди.

3. Интернет тармоғида очик электрон савдо протоколлари(Internet Open Trading Protocol), JEPI (Joint Electronic Payment Initiative) стандарти таҳлил қилинди;
4. Электрон тўлов тизимлари(Онлайн кредит карта тўлов тизими, Электрон чек тўлов тизими, Электрон пул тизими, Электрон тўлов тизимларига асосланган смарт карталар) кўриб чиқилди ва таҳлил қилинди;
5. Ананавий тўлов тизимлари ва электрон тўлов тизимларида ахборот хавфсизлиги масаласи кўриб чиқилди;
6. Интернетда тўловни амалга оширишда канални шифрлаш пратокллари SSL ва TLS таҳлил этилди.
7. Ҳозирда Ўзбекистонда фойдаланилаётган тўлов усуллари тадқиқ қилинди.

II боб. Электрон тўлов тизимларида хавфсизликни таъминлаш

1. Электрон тўлов тизимида хавфсизлик масаласи

Банкларда ва электрон тўлов тизимларида хавфсизликни таъминлаш масаласи ташкилот ёки корпоратив тармоқлар хавфсизлигидан кескин фарқ қилади. Ушбу мураккаблик одатдаги таҳдидлар шунинг билан бирга банк фойдаланувчиларига ва электрон тўлов тизими фойдаланувчиларига қулайлик яратишдаги қийинчиликлардан ташкил топади.

Бундан ташқари ташкилот ва корхоналардаги маълумотлар тор доирада зарур ахборот саналганлиги ушбу ахборотга нисбатан таҳдидни ҳам камайтиради. Электрон тўлов тизимида ёки банкларда эса бундай эмас.

Банкларда ва электрон тўлов тизимларида ахборот хавфсизлигини таъминлашда қуйидагиларни ҳисобга олиш керак:

1. Банкларда ва электрон тўлов тизимларида ахборотлар ҳақиқий пул билан боғлиқ бўлади. Бунинг натижасида эса ўғирланган маълумот ёки ўзгартирилган маълумотлар эвазига шиддий молиявий зарар этказилиши мумкин.
2. Банкларда ёки электрон тўлов тизимларида ахборот мижозларга тегишли бўлганлигидир. Ҳар бир банк ёки электрон тўлов ташкилоти эса ушбу ахборотни махфий сақлаши шарт. Таҳдидларни юзага келиши эса ўз навбатида бу ташкилот ёки банклардан мижозларнинг кетишига олиб келади.
3. Ҳозирда интернет тармоғини ҳаётимизда кенг тарқалиши эса ҳар бир соҳада ишларни амалларни масофадан туриб ажариш имконини беради. Ўз ўрнида банкларда ҳам масофадан туриб пул ўтказмаларини амалга ошириш имконияти мавжудлиги.
4. Банкларда ва электрон тўлов тизимларида ахборот хавфсизлиги юқори даражада бўлиши керак. Бу бир томондан банк ёки ташкилот ахборот, бошқа томондан эса мижоз ахборотини сақлаш учун зарурдир.

5. Банкларда мижозлар учун қимматли бўлган ахборот сақланиши ва бу ахборотга бошқа кўплаб бузғунчилар томонидан бўлган қизиқиш.

Банкларда юзага келадиган жиноятчилик қуйидаги ўзига хос хусусиятларга эга:

- ҳозирда банкларда мавжуд жиноятчиликлар ва таҳдидлар ҳақидаги маълумотлар сирлиги. Жиноятчилик ҳақида элон қилмасликнинг сабаби, мижозларни хавотирга қуймаслик ва бунинг натижасида ўз мавқесини ёқотмаслик;
- одатдаги каби бузғунчи ҳам ўз ҳисоб рақамидан фойдаланиши ва бузғунчиларнинг кўплари ўғирланган пулларни яширишни билишмайди.
- Кўплаб компьютер жиноятчилиги моддий томондан кичкинадир. Улардан келадиган зарар \$10.000 дан \$50.000 гача.
- Муофақиятли компьютер жиноятчилигини амалга ошириш учун кўплаб (бир неча юз) амалларин бажариш кераклиги. Катта миқдордаги пулни ўтказишда кўплаб амалларни бажаралаши.

Электрон тўлов тизимларида ахборот хавфсизилигини таъминлашда қуйидаги асосий икки вазифа қўйилади [17,18,19]:

1. Аналитик вазифа. Бу вазифа режалаштириш ёки ҳисобларни таҳлил қилиш билан боғлиқ. Ушбу вазифа оператив саналмайди ва шунинг учун узоқ вақт олиши мумкин, натижаси эса аниқ мижоз ёки проект билан банк ўртасидаги алоқага тасир қилади. Шунинг учун бу вазифа асосий ахборотни қайта ишлаш жараёни билан ажратилиши керак. Ушбу турдари вазифани бажариш учун кучли ҳисоблаш қурилмалари талаб этилмайди, ўртача ҳисобда умумий қурилма ва жихозларнинг 10-12% га тенг бўлади. Бир муҳим томони эса ушбу вазифани доимий бажарилишидир.
2. Кунлик вазифа. Ушбу вазифалар ҳар кун бажарилиб, улар биринчи навбатда тўловларни амалга ошириш ва ҳисобни тўғирлашдан иборат.

Айнан ушбу жараёни бажаришда тизимнинг асосий ресурси талаб қилинади. Ҳар бир амал қисқа вақтда бажарилиши сабабли, шу жараёнда ҳисоб рақами, пул суммаси ёки мижоз махфий маълумотлари қатъий сир тутилиши шарт.

2. В2С ва С2С тизимларида электрон транзакция хавфсизлиги

Ҳозирги кунда карточкалар билан боғлиқ бўлган уч турдаги таҳдидлар мавжуд:

1. Картани қалбакилаштириш;
2. Картани ёқолиши;
3. Транзакция пайтида ҳирибгарликни вужудга келиши.

Ҳозирга кунда карточкалар билан боғлиқ фирибгарликларнинг 73% дастлвбки икки турга тегишли бўлиб, шу сабабли ҳозирга кўп банклар айнан шу икки муаммони ҳал этишда қаратилган ишларни амалга оширишяпти.

Буларга яққол мисол сифатида микропроцессорларни қалбакилаштиришни (Counterfeit) олишимиз мумкин.

Ҳозирги кунда EMV-карталар статик аутентификацион карталардан ташкил топган (Static Data Authentication).

Бундан ташқари динамик саналган карталар (DDA-карта) ҳам фойдаланилмоқда. Статик аутентификациялаш карталарида эмитент маълумотлари, карта рақами, тартиб рақами, карта эгаси ва ҳ.к сақланади.

Ушбу барча маълумотлар картада очик тарзда сақланади. Статик аутентификация карталари дейилишига сабаб, картадаги маълумотларни ўзгартириш имкони йўқлиги ва бунинг натижасида эмитент рухсатсиз шахсийлаштириш имкони йўқлигидир.

Кўриниб турибдики, бу тоифадаги карталарни қалбакилаштириш қийин эмас. Барча қурилма этарли бўлганда битта пластик карточкани қалбакилаштириш учун ўртача 30 \$ га тенг. Тайёр бўлган картани эса офлайн карта сифатида ишлатиш мумкин. Ушбу ҳолда фойдаланилаётган SDA

микропроцессорли карта этарли эмас. Бунинг учун яна ўғриланган ёки ёқолган карталар керак бўлади.

Булардан фарқли DDA –карталар юқори даражадаги хавфсизликни таъминлайди ва шунинг билан бирга қимматлироқдир. Ушбу турдаги карталарни ҳозирга кундаги нархи SDA-карталарга қараганда 2 марта қиммат, ўртача 2 \$ ва шунга яраша криптографик қўшимча процессор ва 4 Кбайтли EEPROM. Бундан ташқари DDA –картадаги маълумотларни алмаштириш ёки қўчириш фақатгина банк орқали амалга оширилади.

Шулардан келиб чиқиб хавфсизликнинг умумий қоидаларини қўидагича келтириш мумкин:

1. PIN –кодни карта билан бирга сақламаслик. Бундай ҳолатда карта йўқолса бузғунчи карта билан боғлиқ исталган ишини қилиши мумкин.
2. Ҳеч кимга PIN-кодни маълум қилмаслик. Карта номери ёки фойдаланувчи маълумотларини, PIN-кодни ҳеч кимга ошкор бўлмаслиги таъминланиши шарт.
3. Картани бошқа кишиларга бермаслик.
4. Картага ҳар бир фойдаланувчи ўз имзосини қўйиши шарт. Бу эса карта ёқотилган пайтда бузғунчи ундан фойдаланаётганда қўл келиши мумкин, яъни сотувчи томонидан имзо қўйишни сўралиши ва бу билан икки имзони фарқига қараб ажратиш мумкин. Бу ҳолатлар ҳозирда камдан-кам учрайди.

Хавфсиз электрон транзакция пратоколи, SET. SET X.509 стандарти сертификацияларига асосланади. Ушбу стандарт ҳозирга кунда Интернет тармоғида энг ишончли саналган ҳимоя туридан биридир.



10-расм. SET стандарти асосида тўлаш тизими структураси

Юқоридаги расм:

- картага эга шахс-харидор;
- истемолчи банки-истемолчига кредит карточка тақдим этувчи молиявий ташкилот;
- Тўлов шлюзи. Сотувчи банкини бошқарувчи, сотувчидан келган сўровни қайта ишловчи ва харидор банкига тақдим этувчи тизим.
- Сертификациялаш ташкилоти – сертификат берувчи ва уни текширувчи ташкилот қисмларидан иборат.

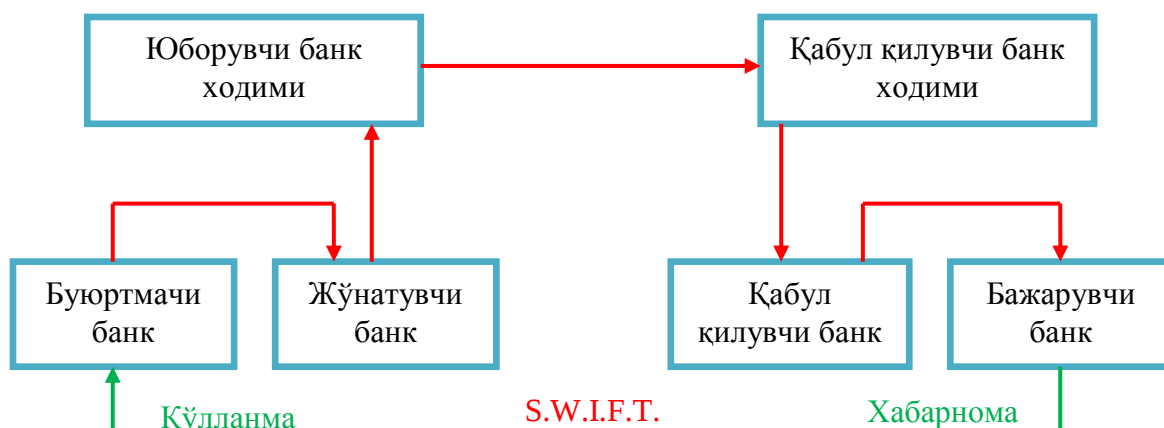
Юқоридаги расмда жараёнлар кетма-кетлиги қуйидагича:

1. Қатнашувчилар(истемолчи, сотувчи ва тўлов шлюзи) сертификацияловчи ташкилотдан сертификат оладилар.
2. Пластик карточка эгаси Интернет магазиндан ўзига керакли товар ёки хизматни танлайди ва сотувчига буюртма беради.
 - Сотувчи ўзининг сертификатини истемолчига кўрсатади.
 - Истемолчи ўз сертификатини сотувчига кўрсатади.
 - Сотувчи тўлов шлюзига бажариладиган амаллар учун сўров юборади. Шлюз тақдим этилаётган ва банкдан олинган маълумотларни солиштиради.

- Текширишдан сўнг шлюз натижани сотувчига юборади.
- Бир қанча вақтдан сўнг сотувчи шлюздан бир ёки бир неча банк амалларини бажаришни сўрайди. Шлюз истемолчи банкидан сотувчи банкка пул ўтказмаси ҳақида сўров юборади.

MasterCard International компаниясининг SPA/USAF стандарти.

MasterCard International корпорацияси истемолчи, сотувчи ва молиявий ташкилот орасидиги кредит ва дебит тўловларини амалга оширишда хавфсизликни таъминлаш мақсадиди янги, Secure Payment Application (SPA)-ечимини ишлаб чиқди. Ушбу тизим MasterCardнинг интернет орқали тўловни амалга ошириш учун ишлаб чиқилган янги тизими бўлиб, тўлов жараёнига қатнашган барча томонларни ҳимоясини таъминлайди. Ушбу хавфсизлик тизими MasterCard корпорацияси томонидан ишлаб чиқилган Universal Cardholder Authentication Field (UCAF) тизимидаги тўлов жараёнлари устида амалга оширилади. UCAF маълумотларни узатиш тизими ҳисобланиб, банк-эмитент ва онлайн сотувчига келган маълумотларни ҳақиқатдан ҳам истесолчидан келганини исботлайди. Ушбу системада 32 битли майдон мавжуд бўлиб, унда савдо маркази ва эквайер маълумотлари шифрланган ҳолда сақланади. У кредит карта маълумотларини савдо маркази ва эквайер орқали шифрланган ҳолатда банк-эмитентга юборади. Эмитент авторизация жараёнини амалга оширади. Шу ҳолда, кичик такомиллашув билан тўлов кафолати олинади. Шунинг учун UCAF MasterCard кредит карталари ва Maestro дебит карталарини қўллаб қуватлайди. Шунини айтиб ўтиш керакки, UCAF эмитентни идентификация қилиш ва ҳимоялаш учун кўплаб тизимларни қўллаб қуватлайди, масалан SPA, смарт-карта ва бошқалар. Ушбу икки тизим UCAF ва SPA ларни биргаликда фойдаланилиши орқали кафолатланган тўловни амалга ошириш тизимини ишлаб чиқиш мумкин [11].



11-расм. Онлайн савдони амалга ошириш схемаси

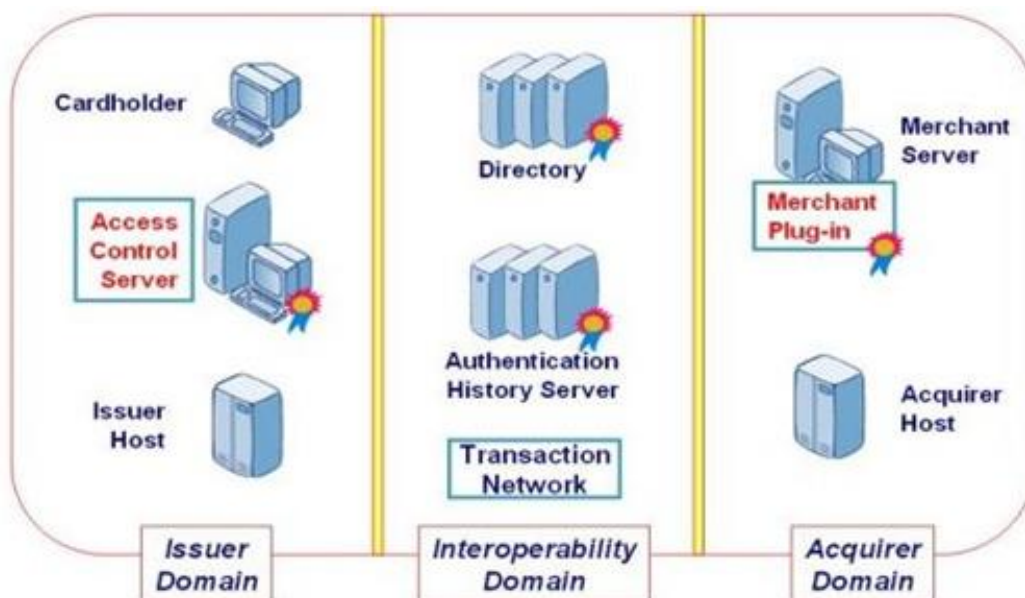
SPA технологияси электрон чекга аналог бўлиб, чек ҳисоб эгасидан номидан олинади. Ушбу технологияда харидор рақамли ҳамёндан (e-wallet SPA-билан ҳамкорликда) фойдаланилиши тавсия этилади. Ушбу харидор MasterCard сайтидан керакли дастурий таъминотни кўчириб олиши шарт. Ҳар сафар истемолчи ҳисоби билан битим амалга оширилган вақтда, 32 битли (Accountholder Authentication Value, AAV) махфий код ҳосил қилинади. Ушбу ҳолда, ҳар бир транзакция вақтида истемолчини текшириш амалга оширилади.

SPA катта молиявий сарфланишни талаб этмайди. Кўплаб ҳимоя тизимлари ушбу технология билан бирлаштирилган.

Ушбу технология сотувчига ҳам истемолчига мавжуд калитга мос калитни беради. Бу эса эмитент томондан идентификациядан ўтган истемолчини тўлов амалга оширилиши тугагунга қадар яна текшириш имконини беради.

Ушбу технологиянинг камчиликлари Visa International ишлаб чиққан 3D-Secure технологиясига қараганда мураккаб ишлаб чиқилгани. Бундан ташқари ушбу хизматдан фойдаланган фойдалунувчи қўшимча дастурий восита кўчириб олиши ва ундан фойдаланиши.

3D-Secure архитектураси. Visa корпарацияси электрон тижоратни шаллантириш ва онлайн транзакцияни ривожлантириш мақсадида 3D-Secure архитектурасини ишлаб чиқди [11, 17].



12-расм. 3-D Secure архитектураси

Cardholder – карта эгаси	Access Control Server – ҳуқуқларни бошқариш сервери	Issuer Host – чиқиш хости	Issuer Domain – чиқиш домени
Directory – маълумотнома	Authentication History Server – аутентификация сервери	Transaction Network – транзакция тармоғи	Interoperability Domain – ўзаро боғлаш домени
Merchant Server – сотувчи сервери	Merchant Plug-in – сотувчи плагини	Acquirer Host – қабул қилувчи хост	Acquirer Domain – қабул қилувчи домен

Ушбу протокъл онлайн транзакцияни амалга оширишда барча томонларни аутентификациядан ўтказди. Ушбу протокъл Интернет тармоғи орқали хавфсиз тўловни амалга ошириш, фирибгарчиликни камайтириш мақсадида фойдаланилган ишончли тизим.

Юқоридаги протокъл қуйидагилардан ташкил топган:

- 3-D Secureдан фойдаланиш барча қисм томонларда молиявий йўқотилишни камайтиришга қўл келади. Фирибгарни имкониятларини камайтиришга олиб келади
- Ушбу протокълдан фойдаланишда фойдаланувчилардан ҳеч қандан аппарат ёки дастурий восита талаб этилмайди.

- Протокол қўшимча ва кенгайтирилган банк-эмитенти мавжуд бўлиб, бу эса фойдаланувчига банк-эквайер ва сотувчи билан алоқаси керак эмаслигини билдиради.
- Протокол электрон тижоратнинг турли кўринишларида, мобиль телефон, чўнтак компьютерлари, рақамли телевизор платформаларида фойдаланилишига имкон беради.
- Ушбу протокол кўплаб техник стандартларга асосланган ва кўплаб халқаро стандартларни қўллаб-қуватлайди.
- Марказлаштирилган архивни аутентификациядан ўтказиш имконияти эса, можороли транзакцияли ҳолатларни олдини олишга имкон беради.

3-D Secure архитектураси. Виза корпорацияси 3 модели янги тўлов тизимини ишлаб чиқди. Асосий ғоя эса, аутентификациялашнинг барча жараёнлари, хавфсиз транзакцияни амалга ошириш учта домен ёки қисмга ажратилади. Домен эмитент вазифаси хизмат кўрсатувчи банк усул ва қоидалар асосида ўзининг савдо марказларини аутентификациядан ўтказди, яъни бу ҳолатда аутентификациялашдаги барча жавобгарлик хизмат кўрсатувчи банкда бўлади. Домен эквайер эса ўзи билан домен эмитент орасидаги маълумот алмашилиш жараёни қоида ва процедуралари аниқлайди.

Карта эгаси домен эмитентда, савдо ташкилоти эса банк эквайерда жойлашган бўлади, улар эса халқаро амалларни бажарувчи домен орқали боғланган.

Ҳуқуқларни бошқариш сервери(Access Control Server) – икки вазифани бажаради:

- 2 рақамли картани 3-D Secure аутентификация қилиш жараёни. Транзакция пайтида ёки аутентификациядан ўтказиш жараёнида муофакиятсиз бўлганда карта эгасини аутентификациялаш. Ушбу амалларни ҳуқуқларни бошқариш серверига, физик серверга

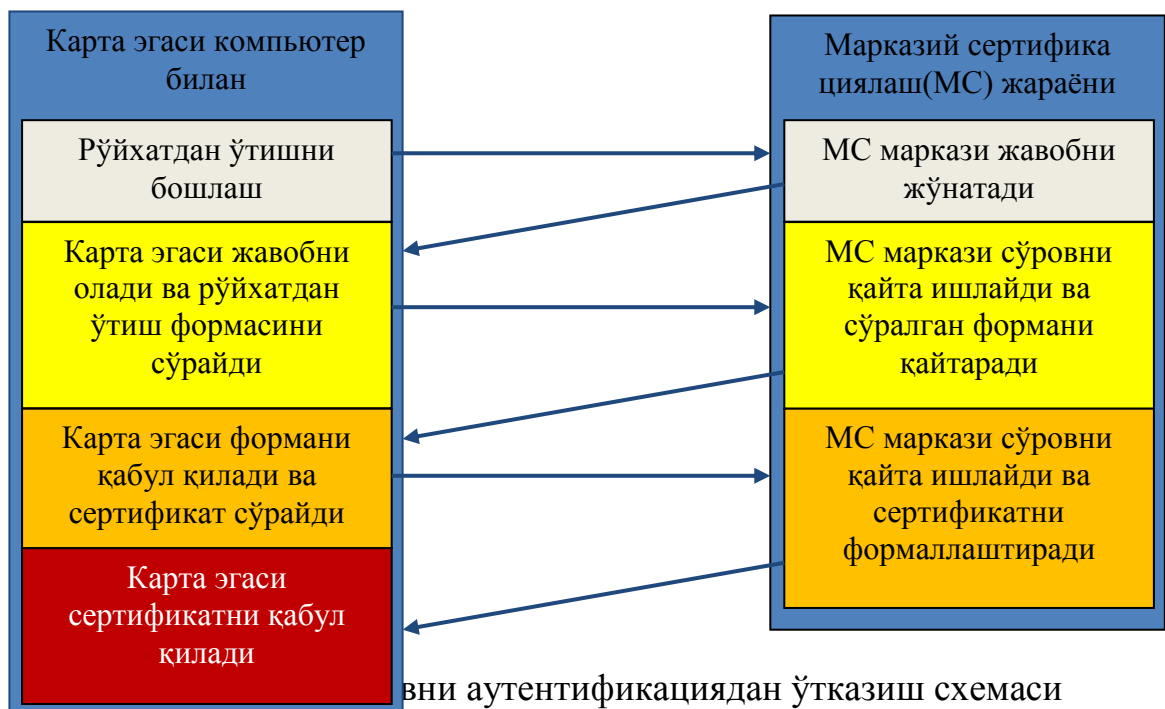
амалга оширилиши керак. Масалан, ушбу серверларнинг ҳар бир аниқланган ораликдаги карталарга хизмат кўрсатади.

- Аутентификация сервери Виза кооперацияси бошқаруви остида бўлиб, унинг вазифаси ҳуқуқларни бошқариш серверидан келган ҳар бир хабарни олиш ва уни ёзиб қўйиш.

Сақланган маълумотлар нусхалари можороли вазиятларда эмитент ва эквайерга жўнатилади.

VisaNet тўлов тизими аутентификация жараёнида қуйидаги вазифани амалга оширади:- эквайердан сўровни қабул қилиш ва эмитентга жўнатиш;- эмитентдан келган жавобни эквайерга жўнатиш.

Тўловни аутентификациялаш жараёни:



Карта эгаси савдони амалга оширади. Карта эгаси савдо қилиш истагини билдирса, дастлаб ўз ҳисоби маълумотларни тақдим этиш керак ёки махсус дастурий воситалардан фойдаланади(масалан, рақамли ҳамён). Ушбу жараён бажарилгандан сўнг, карта эгаси сотувчи серверга(Merchant Server Plug-in) мурожат қилади. Ушбу плагин интернет-магазинда, эквайерда ёки учунчи томонда жойлашган бўлиши мумкин.

Виза маълумотномасига сўров. Сотувчи сервер плагини Виза маълумотномасига хабар жўнатади. Жавоб эса ушбу кредит карта ҳақиқатда

эгасига тегишли ёки эмаслигини аниқлайди. Агар мижоз картаси белгиланган ораликда жойлашган бўлса, Виза маълумотномаси олувчи серверига сотувчи сервер плагини орқали транзакцияни қайтаради. Шундан сўнг сотувчи авторизация сўровини жўнатади.

Карта эгасини аутентификацидан ўтказиш. Сотувчи сервери ҳуқуқларни бошқарувчи серверга аутентификациядан ўтказиш учун сўров юборади. Ушбу сўров истемолчи браузерни ёрдамида амалга оширилади. Ҳуқуқларни бошқариш сервери истемолчи ойнасида киритилган маълумотлар, парол ёки сертификатлар асосида амалга оширилади. Ҳуқуқларни бошқариш сервери истемолчинини ишончли деб топгандан сўнг, жавобни сотувчи серверга жўнатади.

EMV(EuroPay, MasterCard ва Visa) – халқаро стандарт бўлиб, микропроцессори мавжуд банк карталари орқали амаллар бажаради. Ушбу стандарт молиявий жараёнларни хавфсиз бажариш учун, учта компания EuroPay, MasterCard ва Visa томонидан ишлаб ишлаб чиқилди.

EMV стандарт карталаридан фойдаланишда асосий фарқ бу- ихтиёрий тўловни амалга оширишда PIN-кодни талаб этилишидир.

EMV стандарти молиявиё жараёнлар учун банк картаси ва тўлов терминали орасида физик, электрон ва маълумотни боғлиқликни аниқлайди. Мавжуд стандартлар, ISO/IEC 7816 контакт карталар учун, ISO/IEC 14443 контакт бўлмаган карталар учун стандартларига асосланади.

EMV стандартида кенг тарқалган вариантлар қуйидагилар:

- VSDC-VISA;
- MChip-MasterCard;
- AEIPS – American Express;
- J Smart- JCB.

EMV асосий афзаллаги- юқори даражадаги транзакция хавфсизлиги ва офлайн транзакцияда аниқ бошқарувда эгаллиги. Мақсадларидан бири эса – карта имкониятларини ошириш. Юқори даражадаги хавфсизлик эса PIN-код ва криптографик алгоритмлар бардошлиги билан тaminланади.

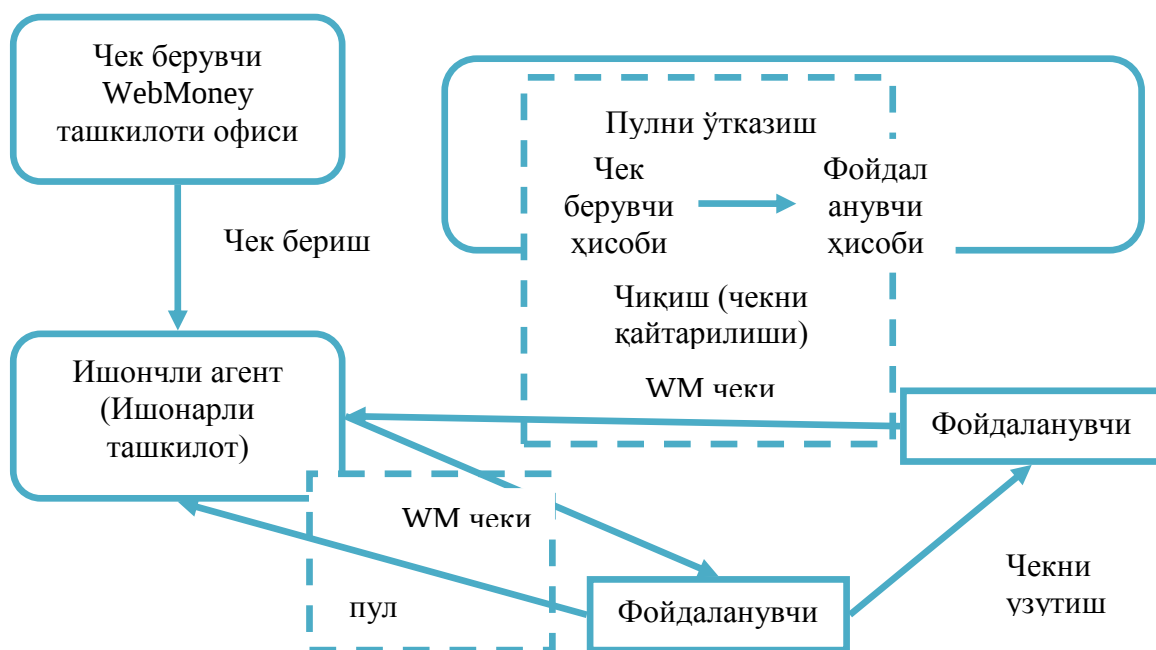
COPS протоколи мақсади сервер сиёсати (Policy Decision Point, PDP) ва (Policy Enforcement Points, PEP) мижоз сиёсати орасида сиёсат маълумотларини алмашишдан иборат.

Webmoney электрон ҳамёни. Webmoney-электрон тўлов тизими саналиб, реал вақт тизимида рўйхатдан ўтилган, яни ягона фойдаланувчи идентификаторига (WMID) эга фойдаланувчилар ўртасида амалга оширилади.

Ушбу тизимдан фойдаланиш учун фойдаланувчи дастурий воситасидан фойдаланилади. Улар қуйидагилар:

- WM Keeper Light – веб-интерфейс орқали;
- WM Keeper Classic – пенсонал компьютерга ўрнатилади;
- WM Keeper Mobile – мобиль воситалар учун.

WebMoney Transfer хавфсиз тўлов тизими комплекс технология саналиб, уч босқичдаги аутентификация мавжуд: WMID, калит ва ҳамён маълумотлари, шахсий рақамли сертификатлар ва тизиматлар ва E-Num. Шунинг учун тизимда маълумот ҳар доим шифрланган кўринишда (RSA алгоритми билан, калит узунлиги 1024-бит ва такрорланмас сеанс калитидан фойдаланилади) юборилади. Тизим алоқани узулиб қолишига бардошли саналади. Фойдаланувчи ихтиёри билан хавфсизлик даражаси белгиланади. Масалан, электрон ҳамёнга рухсатни чеклаш, унга бир IP адресдан ёки чегараланган адресдан мурожат этилишини белгилаш мумкин.



14-расм. «WebMoney Transfer» тўлов тизими

WebMoney Transfer тизимида ҳисоб аноним саналаб, фойдаланувчи қисмда қолади. Фойдаланувчи тизими ўзининг шахсий маълумотларидан ташкил топган рақамли гувоҳнома олиш имкониятига эга. Ушбу гувоҳнома “шаҳодатнома” деб аталади ва у қуйидаги даражаларга эга:

- Псевдоисм шаҳодатнома – тасдиқдан ўтмаган маълумотлар.
- Формал шаҳодатнома – ўзида шу пайтгача текширувдан ўтмаган паспорт маълумотларини қамраб олади. Ушбу шаҳодатнома банк билан амалёт ўташ имконини беради. Фойдаланувчи тўловни киритиши ва чиқаришда почта орқали, банк ёрдамида ва терминаллар ёрдамида амалга ошириши мумкин.
- Бошланғич шаҳодатнома- шахс паспорт маълумотлари текширувдан ўтказилгандан сўнг шаҳодатнома берувчи марказга тақдим этилади. Ушбу шаҳодатномани олиш минимал 1 WMZ қийматидаги суммага тенг. Ушбу шаҳодатнома фойдаланувчига кредит биржалари билан ишлаш имконини беради.
- Шахсий шаҳодатнома –шаҳодатнома берувчи марказдан олинади. Унинг минимал қиймати 5 WMZ. Кўплаб шахсий шаҳодатномалар бошланғичдан олдин:

- Маслахатчи тизимлар ҳолатини олиш;
- Турли тизим сайтларида янгиликларни жойлаштириш имконияти;
- Гувоҳнома беришда шаҳодатнома берувчи марказ дастурларида қатнашиш;
- Судга мурожат имконияти.
- Рўйхатчи шаҳодатнома – энг юқори даражадаги шаҳодатнома саналиб, шаҳодатнома берувчи марказ билан учрашгандан сўнг олиш мумкин. Ушбу шаҳодатномани олиш тизим билан шартнома тузилиши ва 2000 WMZ миқдорда тўлов талаб этилади.

Мобиль алоқа воситалари орқали тўлаш. Сўнги 10 йилликда мобиль алоқа воситаларини ривожланиш кескин кузатила бошлади. Ушбу имконият эса ўз навбатида барча соҳалар қатори электрон тўлов соҳасида ҳам катта ўзгаришларни амалга оширди. Бу имкониятлар қаторига мобиль-банкнинг ва мобайл алоқа воситалари орқали тўлашни олишимиз мумкин. Мобиль алоқа воситаси ёрдамида тўлаш қолган электрон тўловлар орасида ажралиб туради. Ушбу тўлов тури орқали амалга оширилган амаллар эса йил сари ортиб бормоқда [24].

Мобиль алоқа воситаси орқали тўловни амалга ошириш қуйидаги 4 та методга асосланади:

- SMS (Short Messaging Service) орқали;
- Тўғридан-тўғри мобиль тўлов;
- Мобиль веб тўлов(WAP);
- Алоқасиз NFC(Near Field Communication).

SMS (Short Messaging Service) орқали тўлов. Ушбу тўлов усулида истемолчи тўлов сўровини SMS, USSD кўринишда жўнатади ва тўлов телефон ҳисобидан ёки онлайн ҳамёндан амага оширилади. Сотувчи келган сўровни қабил қилади ва хизматни амалга оширади [24].

Ушбу тўлов усулида одатда маҳсулотлар сотиб олишда эмас, рақамли хизматларни амалга оширишда фойдаланилади. Шунинг учун ҳам рақамли

хизмат MMS(Multimedia Messaging Service) орқали этказилади. Бу хизматларга қўшиқлар, расмлар ёки шунга ўхшаш рақамли маълумотлар.

SMS орқали тўлов асосан Осиё ва Европа давлатларида оммабоп саналган ва ҳозирда ушбу хизмат бошқа ривожланган мобиль веб тўлов, мобиль тўлов мижоз дастурларига асосланган (Java ME, Android, IOS) ва тўғридан-тўғри тўлов усуллари орқали сиқиб чиқарилмоқда.

SMS орқали тўлов усулининг камчилиги қуйидагилар:

- Ишончилиқ даражаси паст. Агар хабар йўқолса транзакция осонгина йўқотилади.
- Паст тезлик. Хабарни жўнатиш узоқ вақтни олади ва хабар сотувчига кеч етиб келади. Харидор эса тез кўрсатишни талаб этади.
- Хавфсизлик. SMS/USSD сўровлари радио тўлқин тугаш жойига қадар шифрланган ҳолда бўлади, кейин эса очик ҳолатда ўтади.
- Қимматлилиқ. Ушбу тўлов турида кўплаб хизматлар қиммат, яъни қисқа хизматдан фойдаланиш учун, юборилган MMS хабар учун олинган хизмат ҳақи. Ушбу қийматлар эса фойдаланувчи ҳисобидан олинади.
- Тўлов суммасининг камлиги. Операторлар томонидан барча амалиётни кузатиб борилиши. Натижада эса кўплаб сотувчи ташкилотлар ушбу хизматдан фойдаланмасликка олиб келади.

Тўғридан-тўғри мобиль тўлов. Ушбу усулда фойдаланувчи электрон коммерция сайти ғазналарида тўлашда фойдаланиши мумкин. Масалан, онлайн тарзда ўйналадиган ўйинлар. Икки факторли аутентификациядан фойдалангандан сўнг, PIN код ва тасодифи сон киритилади ва таклиф этилган сумма олиб қолинади. Бу муқобил тўлов тури бўлиб, ҳеч қандай кредит ёки дебит карта талаб этилмайди [24].

Ушбу турдаги тўлов тури Осиё давлатларида кенг тарқалган бўлиб, қуйидаги афзалликларга эга:

- Хавфсизлик. Икки факторли аутентификация ва хавфларни бошқариш тизими ёлғонни олдини олади.
- Қулайлилик. Ҳеч қандай рўйхатдан ўтиш ёки дастурий восита талаб этилмайди.
- Тезкорлик. Асосан транзакцияларнинг 10 сек кам вақтда амалга оширилиши.
- Ишботланганлик. Осиёда 70% ортиқ рақамли хизматлар учун айнан ушбу тўлов туридан фойдаланиши.

Мобиль веб тўлов. Ушбу тўлов усулида истмолчи веб саҳифадан ёки кўчириб олинган ва ўрнатилган махсус дастурий воситаладан фойдаланади. Ушбу тўлов тизими WAP(Wireless Application Protocol) пратоколидан фойдаланади ва ушбу пратоклда мавжуд камчилик ва афзалликларга эга. Афзалликлар қуйидагиларни ўз ичига олади [24]:

- Давомли савдо. Истемолчига тавар ва хизматларни танлашда қулайлик яратади.
- Тезкор ва қулай бўлганлиги учун истемолчилар томонидан афзал кўрилиши.
- Фойдаланишда қулайлиги.

Ушбу тўловни амалга оширили фақат фойдаланувчи телефон рақами ҳисобидан олинади. Натижада эса ушбу тўлов тизимида кредит, дебит ёки олдиндан рўйхатдан ўтиш тўлов тизимларига бўлган талаб ортади.

Тўғридан-тўғри оператор тўлови. Ушбу усул WAP тўлов усули ҳам деб аталади ва қуйидаги қулайликларга эга:

- Оператор дастлаб истемолчи билан келишиб тўловни амалга оширади. Кейин бўлган тўловлар эса уларга қўшилиб борилаверади.
- Тўлов тезда амалга оширилади.
- Истемолчи идентификатори ва тўлов ҳисоби ҳимояланади.
- Яхши ривожланиш кўрсаткичига эга.
- Сотиб олувчилар истемолчи хизматларини камайтиради.

Камчилиги эса бошқа тўлов тизимларига нисбатан кам тарқалганлиги.

Кредит карта ёрдамида тўлаш. Мобиль алоқаси ёрдамида кредит карта орқали тўлов амалга оширилади. Ушбу жараён одатий саналиб, мобиль алоқа орқали юборилган ҳар бир маълумот тўловни амалга оширилиш даражасини камайтиради.

Онлайн ҳамёнлар. Онлайн ташкилотлар, PayPal, Amazon Payments ва Google Wallet тўлов тизимларида мобиль алоқа воситасидан фойдаланади. Ҳозирда ушбу жараён шакллантирилмоқда.

Тўлов биринчи марта қуйидаги тартибда амалга оширилади:

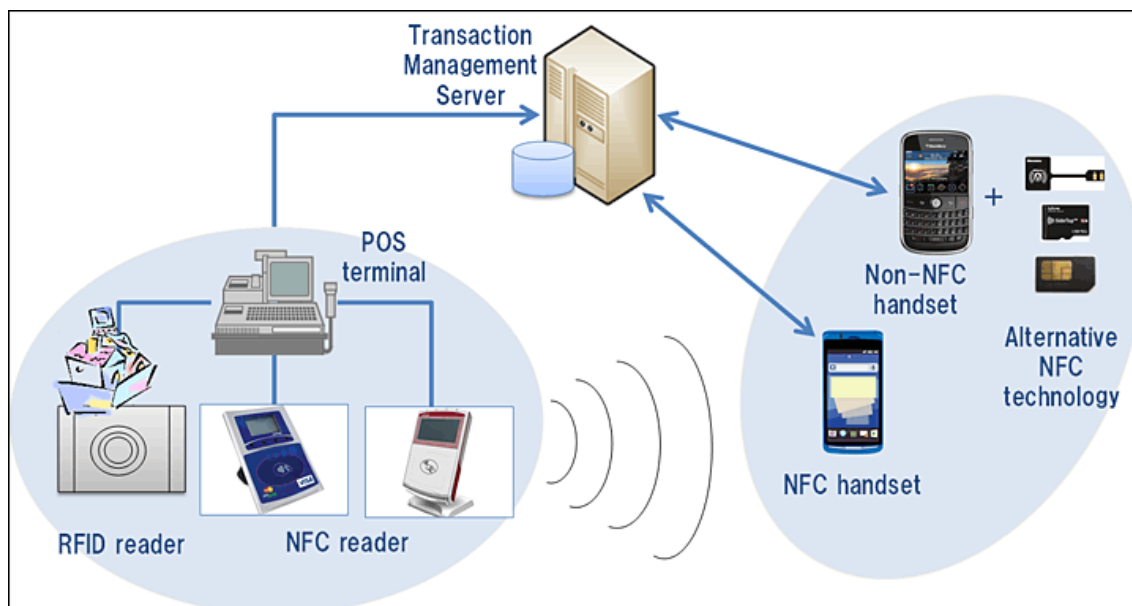
- Фойдаланувчи рўйхатдан ўтади ва телефон рақамини ҳам киритади. Онлайн савдо ташкилоти эса SMS орқали PIN кодни юборади.
- Фойдаланувчи PIN кодни ва аутентификация рақамини киритади.
- Фойдаланувчи кредит карта маълумотларини киритади ёки керакли бўлса бошқа тўлов турини танлайди.

Кейинги тўловлар:

- Фойдаланувчи аутентификация учун PIN кодни киритади ва тўловни тасдиқлайди.

Ушбу тўлов тизимида фақат PIN коддан фойдаланилиши хавфсизлик даражасини туширади. Амалда эса тизимни тўғридан-тўғри ёки алоқа компаниялари билан бирлаштирилиши шарт ва мобиль веб тўлов тизимида амалга оширилиши шарт.

Алоқасиз NFC(Near Field Communication). Near Field Communication смартфонлар ёки шунга ўхшаш бўлган қурилмалар учун ишлаб чиқилган махсус стандарт бўлиб, қурилмалар бир-бирига яқинлаштирилганда радио сигнал орқали бир-бири билан боғланади. Алоқасиз тўлов тизимлари хавфсиз тўловни амалга ошириш учун радио тўлқин майдонидан фойдаланадиган дебит, кредит ёки смарт карталар бўлиши мумкин [23, 24].



RFID(radio-frequency identification) reader-

радио тўлқин қабул қилувчи

NFC handset – NFC мавжуд аппарат

NFC reader – NFC тизимини ўқиш.

Non-NFC handset – NFC мавжуд бўлмаган аппарат

POS(Point of Sale) terminal – электрон аппарат-дастурий қурилма

Alternative NFC technology – Муқобил NFC технологияси

Transaction Management Server – транзакцияни бошқарувчи сервер

15-расм. NFC тўлов тизими

Ушбу усулда тўлов қуйидагича амалга оширилади:

- Дастлаб қайси банк NFS мавжуд телефонларда карта рқали тўловни амалга ошириш имконияти мавжудлиги текширилади;
- Ушбу банкдан NFS мавдуд телефон харид қилинади;
- Ушбу банкда NFS ли телефон билан карта рўйхатдан ўтилади;
- Тўлов картаси маълумотларини юклаб олинади;
- Тўлов картани NFS телефонида уланади ва шундан сўнг тўловни амалга ошириш имкониятига эга бўлинади.

Ушбу тўлов усулида хавфсизлик масаласи одатдаги каби PIN код асосида амалга оширилади.

3. Электрон тўлов стандартлари таҳлили

Ҳозирги кунда келиб барча молиявий катта ташкилотлар ўзлари учун янги электрон тўлов архитектураларини ишлаб чиқишмоқда ва тақдим этишмоқда. Электрон тўлов стандартларини кўплиги ҳар бир фойдаланувчидан улардан тўғри танлов асосида фойдаланиш керак эканлигини англатади.

Шуларни ҳисобга олиб ушбу бўлимда ҳозирда кенг тарқалган тўлов тизимларидан бири саналган мобиль қурилма воситаси ёрдамида тўловни амалга оширишда мавжуд заифликлар ва уларни бартараф этиш чоралари қуйидаги жадвалга келтирилган [15].

3-жадвал

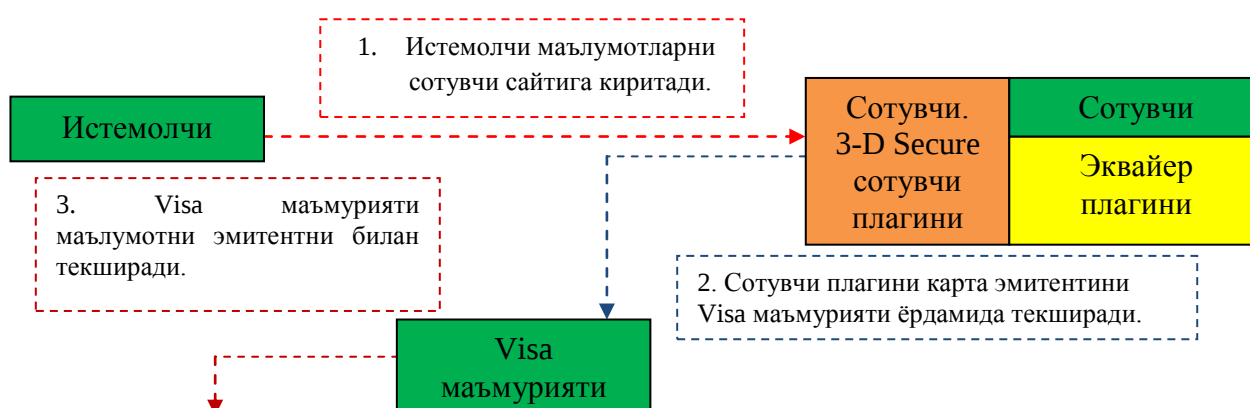
Мобиль тўлов тизимида таҳдидлар

Тури	Заифлик	Таҳдид	Хавф	Ҳимоя чораси
Фойдала нувчи	Телефон ва савдо нуқтаси (POS, NFC reader) опрасидаги ҳаво орқали боғланишда	Трафикни ушлаб қолиш	Маълумотни ошкор этилиши, ҳужумни қайтарилиш, ўғирликка ўхшаши	Ишончли платформа модули, хавфсиз протокол, шифрлаш
Фойдала нувчи	Фойдаланувчи томонидан бузғунчи дастурларни билмасдан ўрнатилиши	Аутентификация маълумотларини кўчириб олинган дастур орқали ушлуб қилиниши	Аутентификация параметрларини ўғирланиши, маълумотни ошкор бўлиши, транзакцияни бекор этилиши	Фойдаланувчи(PIN) ва дастурни(учунчи томон орқали ЭРИ билан) аутентификациядан ўтказиш, ишончли платформа модули
Фойдала нувчи	Икки факторли аутентификацияни мавжуд эмаслиги	Фойдаланувчини никоблаш	Алданган транзакция, правайдер мажбурияти	Икки факторли аутентификация
Фойдала нувчи	Мобиль телефонни алмаштирилиши ёки ёқотилиши	Созлаш ва ўрнатишнинг мураккаблиги	Мос технология ларнинг камлиги, аниқ бўлмаган хавфсизлик	Содда фойдаланувчи интерфейси, ишончли платформа модулида хавфсиз параметрларни ишончли томон орқали ўрнатиш
Фойдала нувчи	Смартфонни интернет орқали жойлашувини аниқлаш имконияти	Мобиль қурилмалардаги бузғунчи дастурлар, сотувчи/харидор фойдаланган ҳимоя	Маълумотларни ошкор бўлиши, фойдаланувчини ошкор бўлиниши	Телефонни аниқлаш тизимини бошқариш, криптографик ҳимоя

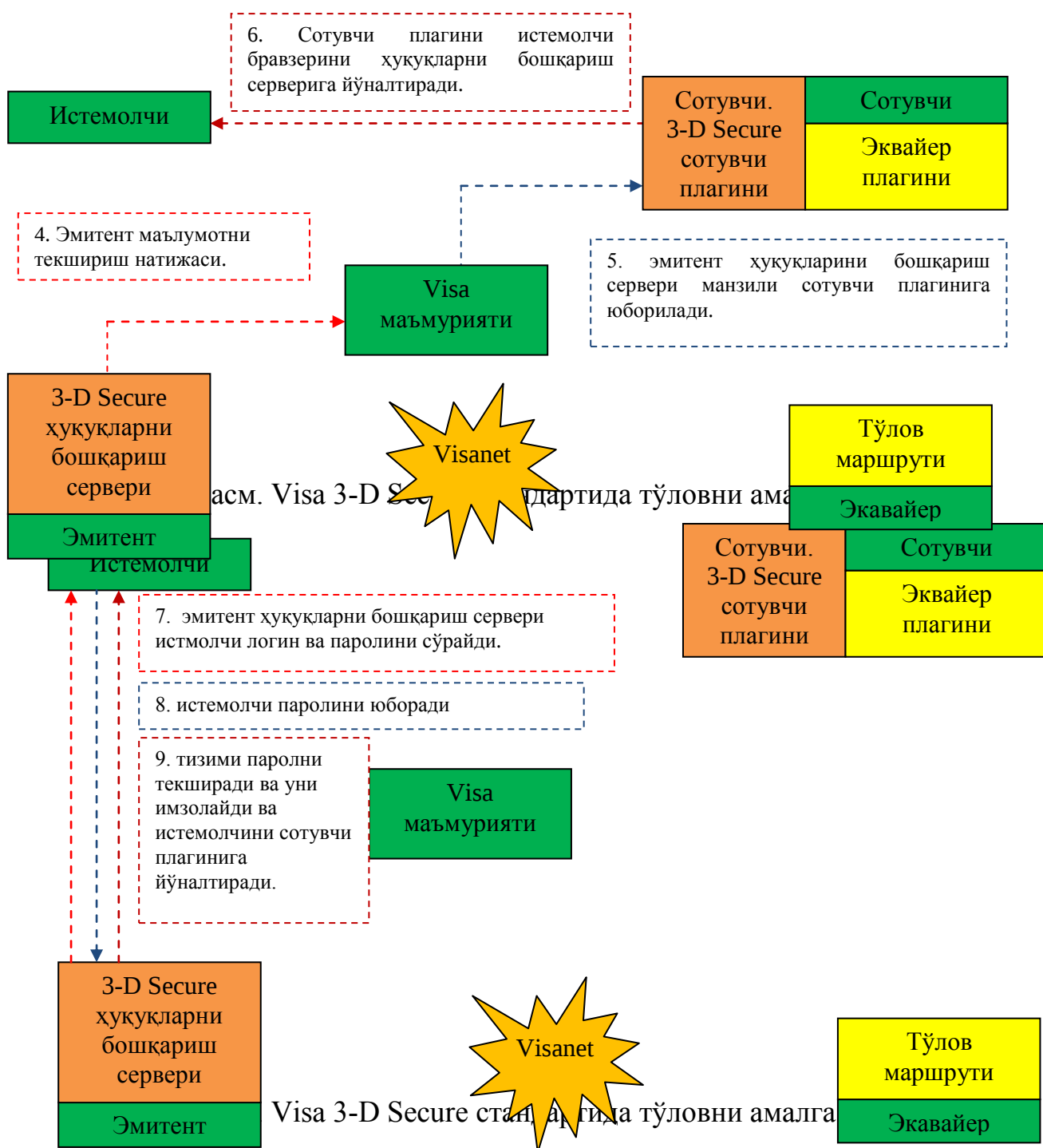
		воситасини заифлиги		
Хизмат кўрсатувчи правайдер	Савдо нуктасида ҳаво орқали боғланиш	Кам талабли савдо нуктаси апаратида бузғунчи қисмларни ортиши	DOS(Denial of Service) хужуми	Қабул қилувчи қурилмаларда филтерлашни амалга ошириш (NFC да)
Хизмат кўрсатувчи правайдер	Сотувчи томонда савдо нуктаси қурилмаси жойлашуви	Ниқоблаш хужумлари, савдо нуктасини қалбакилаштириш	Хизматни ўғирланиши, қайтарилиши, хабарни алмаштирилиши	Савдо нуктаси апаратида харидорни текшириш, хабарни аутентификациялаш, текширилган авторизация ва ҳисоб
Хизмат кўрсатувчи правайдер	Мобиль қурилмаларда рақамли бошқарувнинг камчилиги	Мобиль қурилма эгаси ташкил этувчиларни(видео, кўшик, ўйин) ноқонуний тачсимлангани	Ташкил этувчиларни йўқолиши, рақамли қалбакилаштириш, истемолчи ва хараидорни қондиришда кам қиримдан фойдаланиш	Мобиль қурилмаларда рақамли бошқарувнинг криптографик ҳимояси,
Хизмат кўрсатувчи правайдер	Транзакцияни амалга оширишда GSM шифрлаш тизимида заифлик, SMS маълумотларини тармоқда очиклиги	Хабарни ўзгартирилиши, транзакцияни қайтарилиши	Контент ёки хизматни йўқолиши, фойдани йўқолиши, ноқонуний пул трансферлари	Кучли крипторгафик протокол, SMS хабарини аутентификациялаш, шифрлаш

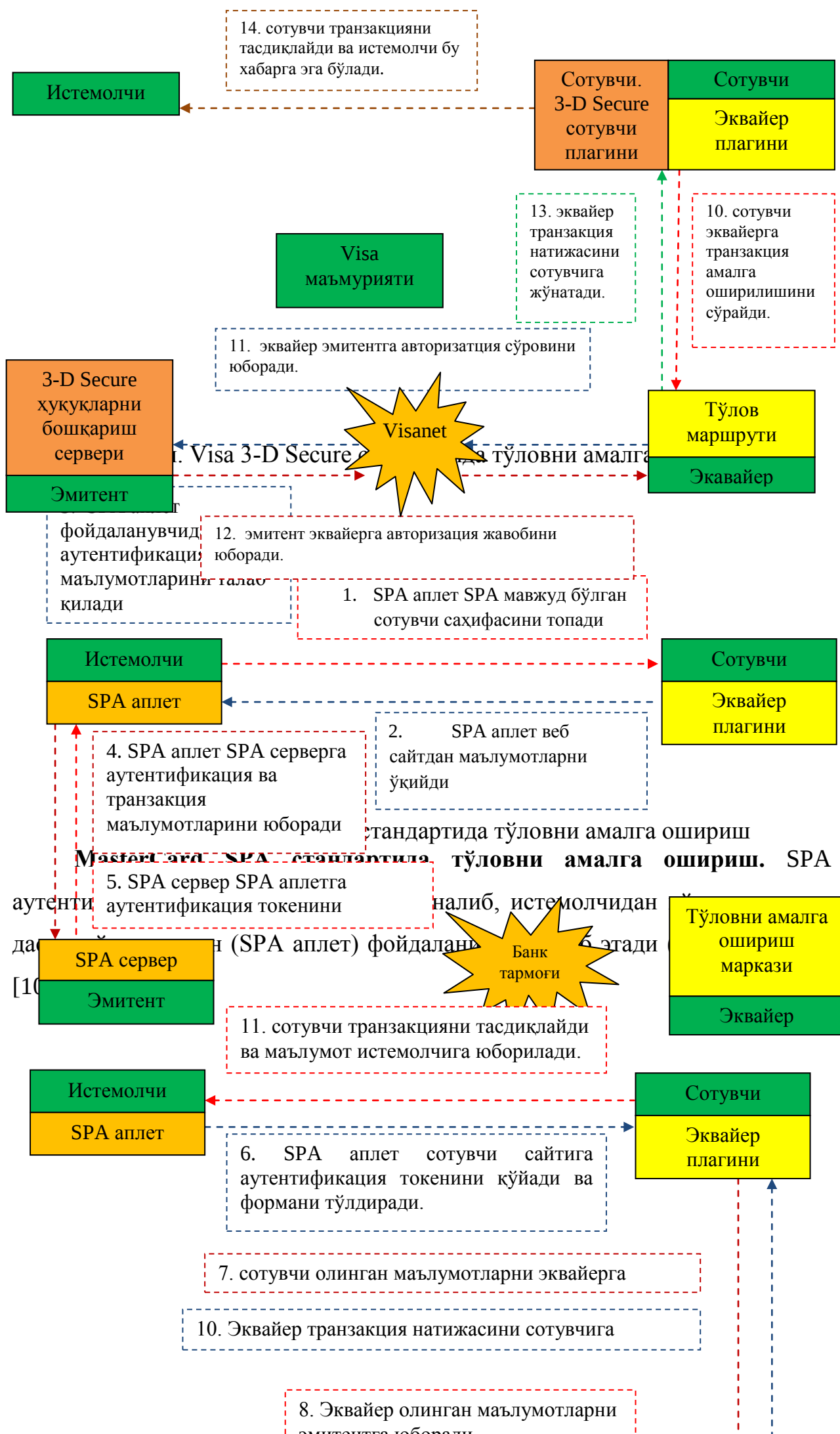
Юқорида келтириб ўтилганидек ҳозирги кунда янги яратилган ва бардошли саналган MasterCard Secure Payment Application ва Visa 3-D Secure стандартлари ҳақида тўхталган эди. Қуйида эса ушбу икки стандартнинг таҳлили келтирилган.

Visa 3-D Secure стандартида тўловни амалга ошириш. Ушбу тизим аутентификация тизими ёки тўлов тизими саналмай, шунчаки учта томонларни бир-биридан ажратиш технологиясидир [10].



16-расм. Visa 3-D Secure стандартида тўловни амалга ошириш





21-расм. MasterCard SPA стандартида тўловни амалга ошириш

Қуйида эса ушбу икки стандартнинг қиёсий таҳлили келтирилган [10].

4-жадвал

Visa 3-D Secure ва MasterCard SPA тўлов тизимлари қиёсий таҳлили

Хусусият	Хусусият ташкил этувчиси	Visa 3-D Secure	MasterCard SPA
Истемолчига боғлиқ бўлган	Дастлабки рўйхатдан ўтиш	Онлайи тарзда амалга оширилади ва 2.5 мин вақтни олади.	Интернет тармоғидан кўчирилган дастурий восита асосида амалга оширилади. Вақти кўшчириш вақтида боғлиқ. Камида 3-4 минут.
	Сотиб олиш	Тўловни амалга ошириш жараёнида қўшимча 10 сўров юборилиб, тўлов текширилиб турилади. Тўлаш вақти 10-15 сек.	Апплетдан фойдаланиш натижасида юбориладиган сўровлар камаяди ва кўп савдо амалга оширилганда қайта аутентификацияни сўрамайди.
	Жойлашувга боғлиқлиги	Бу тизимда тўловни амалга оширишда истемолчи жойлашган жойни фарқи йўқ.	Апплет ҳар бир фойдаланувчи учун ягона бўлганлиги сабабли ихтиёрий жойда фойдаланиб бўлмайди.
	Қўшимча хизматлар	Онлайн тизимда ишлагани сабабли қўшимча имкониятлари йўқ.	Истемолчига қўшимча, онлайн транзакция маълумотлари, сотувчи сайти манзили ва ҳ.к.
	Эмитентни амалга оширилиши	Эмитентни амалга оширишда ҳеч	Ҳар бир эмитент SPA сервердан рўйхатдан

Эмитент билан боғлиқ		қандан дастурий, аппарат воситалар талаб эитлмайди.	ўтиши ёки ушбу серверни ўзига ўрнатиши лозим.
	Фойдаланувчилар кўмаги	Асосан бу вазифани кўпинча эмитент бажаради	Бу вазифа аплет зиммасига тушади ва у кўплаб имкониятлар беради.
	Эмитент жавоби	Кўплаб жавоблар бўлиб, улар кредит карта рақами, аутентификация ҳолати, нарх. Асос маълумотлар	Эмитент кўплаб куқиқлар мавжуд, яъни транзакцияни ўзгартириш, қисқартириш
Сотувчи билан боғлиқ	Сотувчи амалга оширадиган жараёнлар	Сотувси плагини билан бирга амалга оширилади ва бу эса барча жойда ундан фойдаланишни кафолатламайди.	Ортиқча плагин талаб этмайди ва ўртага турган 3-шахс хужумига бардошли.
	Сотувчига жавоб	Транзакция ҳақидаги маълумотлар Payment Gateway орқали тўлиқ олинмайди.	Барча транзакция ҳақидаги маълумотлар бир жойда сақланади ва олинади.
	Давомий талаблар	Сотувчи плагини янгиланишни сўрайди.	Янгиланадиган восита йўқ.
Эквайер билан боғлиқ	Технологик амалга оширилиш	Эквайер тўлов амалга оширувчи марказ билан амалга оширади.	Эквайер тўлов амалга оширувчи марказ билан амалга оширади.
Архитектураси бўйича	Марказлашган ёки тақсимланган	Марказлашган	Тақсимланган
Хавфсизлик архитектураси бўйича		Аутентификация ва авторизатция жараёнлари алоҳида-алоҳида жараёнлар	Битта жараённинг ўзида ҳам аутентификация ҳам авторизациядан ўтилади.

II боб бўйича хулосалар

- Электрон тўлов тизимларида хавфсизлик масаласи кўриб чиқилиб, уларга қўйилган талаблар, вазифалар ва ўзига хос хусусиятлар келтирилди.
- B2C ва C2C тизимларида мавжуд таҳдидлар таҳлил этилди.
- Хавфсиз электрон транзакция протоколи саналган SET протоколи таҳлил этилди.

- MasterCard International компаниясининг SPA/USAF стандарти ишлаш усули кўриб чиқилди.
- Ҳозирга кунда SPA/USAF стандартига рақабатдош саналган Visa 3-D Secure стандарти тадқиқ этилди.
- Webmoney электрон тўлов асосида тўловни амалга ошириш усули таҳлил этилди.
- Мобиль алоқа воситалар ёрдамида электрон тўловни амалга ошириш усуллари тадқиқ ва таҳлил этилди.
- Электрон тўлов стандартлари саналган SPA/USAF ва Visa 3-D Secure стандартлари ўзаро қиёсий таҳлил этилди.
- Мобиль воситадан фойдаланган ҳолда тўловни амалга ошириш тизимларида мавжуд камчиликлар таҳлил этилди ва уларни бартараф этиш усуллари таклиф этилди.

III боб. Интернет магазинда тўлов тизими хавфсизлигини таъминлаш

1. Электрон тўлов тизимининг криптографик ҳимоя воситалари таҳлили

Юқорида кўриб ўтилганидек, электрон тўлов тизимлари хавфсизлигини таъминлашда криптографик алгоритмлардан кенг фойдаланилди. Ушбу алгоритмларни қуйидаги турларга ажратиш мумкин:

- симметрик шифрлаш алгоритмлари;
- ассиметрик шифрлаш алгоритмлари;
- электрон рақамли имзо алгоритмлари;
- калит узатиш протоколлари;
- хэш функциялар.

Ушбу криптографик алгоритмлар ёрдамида электрон тўлов тизимида қуйидаги амалларни бажаришда фойдаланилади:

- транзакция маълумотларини шифрлаш;
- калитларни узатиш;
- маълумотни яхлитлигини таъминлаш;
- аутентификациялаш ва ҳ.к.

Шуларни ҳисобга олган ҳолда электрон тўлов тизимларида криптобардошли алгоритмлардан фойдаланиш юқори самара беради. Қуйида эса ҳар бир турдаги алгоритмларнинг таҳлили келтирилган.

Симметрик алгоритмларнинг таҳлили. Симметрик алгоритмлар шифрлаш ва дешифрлаш жараёнида битта калитдан фойдаланади. Ушбу шифрлаш алгоритмлари шифрлаш ва дешифрлаш жараёнида асимметрик алгоритмларга қараганда юқори тезликка эга, калит узунлиги эса бир хил бардошлиликка эришганда кичикдир. Бу эса симметрик шифрлаш алгоритмларидан катта ҳажмдаги маълумотларни шифрлашда фойдаланиш катта ютуқ беради. Қуйида айнан электрон тўлов протоколларида фойдаланилган симметрик алгоритмларнинг қиёсий таҳлили келтирилган.

5-жадвал

Шифрлаш алгоритмлар таҳлили

Хусусият	DES	AES	Blowfish
Муаллифи	IBM ташкилоти	Винсент Рижман ва Хуан Даймен	Брюс Шнайер
Калит узунлиги (бит)	56	128, 192, 256	32-448, ўзгарувчан
Кириш блок узунлиги (бит)	64	128	64
Раунд сони	16	10, 12, 14	16
Математик асоси	XOR, суриш ва ўрин алмаштириш	Кўпхадлар устида амаллар, XOR, суриш	MOV, ADD, XOR
Яратиш асоси	Фейстел тармоғи	SPN тармок	Фейстел тармоғи
Энг катта натижага эришган ҳужум тури	Brute-force ҳужуми	Side-channel ҳужуми	Калит заифлигига асосланган ҳужум

Қуйида ушбу алгоритмларнинг крипто таҳлил тизими саналган Crypto++ дастурий таминоти орқали таҳлил қилинганда олинган натижалар берилган.

6-жадвал

Шифрлашдаги тезликлар бўйича таҳлил

Алгоритм	Шифрланадиган маълумот (МБ)	Вақт	МБ/Сек
Blowfish	256	3,976	64,386
Rijndael(128)	256	4,196	61,01
DES	128	5,998	21,34
3DES	128	6,159	20,783

Ассиметрик шифрлаш алгоритмлари таҳлили. Симметрик алгоритмлардан фарқли равишда ассиметрик алгоритмлар электрон тўлов пратокollarида маълумотларни шифрлаш учун эмас, асосан симметрик шифрлаш алгоритмлари калитларини алмашилишида, электрон қарамли имзо алгоритмлари орқали аутентификациядан ўтказишда фойдаланилади. Ҳозирда ассиметрик алгоритмлар орасида кенг фойдаланилаётгани RSA ва эллиптик эгри чизиқларга асосланган ассиметрик алгоритмлар кенг фойдаланилади. Шуларни ҳисобга олган ҳолда қуйида ушбу икки алгоритмларнинг қиёсий таҳлили келтирилган [7,8].

RSA ва эллиптик эгри чизиққа асосланган алгоритмларнинг калит узунликлари бўйича таҳлили

7-жадвал

Очиқ калитли алгоритмлар таҳлили

RSA	ECC
512	113
768	136
1024	160
2048	282
4096	409

8-жадвал

RSA ва эллиптик эгри чизикқа асосланган алгоритмларнинг хусусиятлари бўйича таҳлили

	RSA	ECC
Умумий параметрлар	-	Қийин. Тавсия этилган параметрлар
Калит генерацияси	Ўзгарувчан. 0.2 с-14 мин. 1024 бит калит: 2.8 сек	0.054 с- 1.4 мин. 161-бит калит:0.09 сек
Шифрлаш	0.02 сек-6.7 сек 1024 бит калит, $e=65537$:0.025 сек	0.05 сек-2.8 мин, 163 бит калит, 2048 байт мал:0.12 мин
Дешифрлаш	0.03сек-4.45 сек 1024 бит калит:0.13 сек	0.03 сек-1.55 мин 163 бит калит, 22 байт мал:0.05 сек
ЭРИ да имзолаш	Дешифрлаш	Дешифрлаш
ЭРИ да имзони текшириш	Шифрлаш	Шифрлаш

Хэш функциялар. Хэш функциялар – ихтиёрий узунликдаги кириш маълумотини чиқишда белгиланган узунликдаги хэш қийматга айлантириб берувчи бир томонлама функцияларга айтилади. Хэш функциялар криптография ва замонавий ахборот хавфсизлиги соҳасида маълумотларни тўлалигини текширишда фойдаланилади. Электрон тўлов тизимлари пратокollarида ҳам истемолчи картаси маълумотларини банк-эмитентга тўлиқ этказиш учун фойдаланилади. Қуйида эса ҳозирда кенг фойдаланилаётган хэш функциялар қиёсий таҳлили келтирилган[7].

9-жадвал

Хэш функциялар таҳлили

	Хешланади ган матн узунлиги	Кириш блокнинг узунлиги	Хэш қиймат узунлиги	Ҳар бир блокни хэшлаш қадамлари сони
ГОСТ Р 34.11-94	Ихтиёрий	256	256	19
MD 2	Ихтиёрий	512	128	1598
MD 4	Ихтиёрий	512	128	72
MD 5	Ихтиёрий	512	128	88
SHA-1	$<2^{64}$	512	160	80
SHA-256	$<2^{64}$	512	256	64
SHA-384	$<2^{128}$	1024	384	80
SHA-512	$<2^{128}$	1024	512	80

СТБ 1176.1 – 99	Ихтиёрий	256	$142 \leq L \leq 256$	77
O'z DSt 1106 : 2006	Ихтиёрий	128, 256	128, 256	16b+74, 16b+46, Бу ерда b-блоклар сони

Электрон рақамли имзо алгоритмлари. Электрон тўлов тизимларида истемолчини аутентификациядан ўтказишда кўплаб усуллар ва протокollar фойдаланилади. Ушбу усуллар асосида эса электрон рақамли имзо алгоритмлари ётади. Электрон рақамли имзо алгоритмларининг асосий мақсади фойдаланувчиларни банк-эмитент билан алоқасида аутентификациядан ўтказиш. Электрон рақамли имзо алгоритмлари асосида маълумотларнинг хэш қийматларини ассиметрик шифрлаш алгоритмлари ёрдамида шифрлашдан иборат. Қуйида кенг фойдаланилаётган электрон рақамли имзо алгоритмлари таҳлили келтирилган [7,8].

10-жадвал

Электрон рақамли имзо алгоритмлари таҳлили

Белгилар	O'z DSt 1092:2005 O'z DSt 1092:2009	DSA	ГОСТ Р 34.10-2001
Алгебраик структура	Параметрли алгебра (параметрли чекли мультипликатив группа)	Чекли оддий майдон	Чекли оддий майдонда аниқланган ЭЭЧ
Модул тип ва ўлчамлари	Туб сон $p > 2^{255}$ (Афзаллиги юқори тезкорликда)	Туб сон $2^{511} < p < 2^{1024}$	Туб сон $p > 2^{255}$
Процедура-ларда фойдаланилган асосий амаллар	1. Параметрли кўпай-тириш 2. Параметр билан даражага ошириш 3. Параметр билан тескарилаш 4. Тескарилаш	1. Кўпайтириш 2. Қўшиш 3. Даражага ошириш 4. Тескарилаш	1. Қўшиш 2. Инкор 3. Кўп марталик қўшиш 4. Конкатенация (Камчилиги амалларнинг мураккаблигида)
Даража асоси тип	Махфий – g (Афзаллиги дискрет логарифмлаш масаласини қўйиш мураккаблигида)	Ошкора – g (Камчилиги дискрет логарифмлаш масаласини қўйиш осонлигида)	Ошкора нукта P (Камчилиги эллиптик эгри чизиқларда дискрет логарифмлаш масаласини қўйиш осонлигида)
ЭРИ узунлигини қисқарти-ришга ёнда-шув	Фактор(($p-1$) нинг туб кўпайтувчиси)дан фойдаланиш	Фактордан фойдаланиш $2^{159} < q < 2^{160}$	Циклик группанинг тартибидан

	$2^{254} < q < 2^{256}$		фойдаланиш $2^{254} < q < 2^{256}$, q - группа тартиби
Ёпиқ калит шакли	Учлик (x, u, g) (Афзаллиги махфийлик даражаси ошмишида)	Параметр x	Параметр d
ЭРИ шакли	Жуфтлик (r, s) $\mu=0$ да, учлик (r, s, u_1) $\mu=1$ да (Камчилиги $\mu=1$ да)	Жуфтлик (r, s)	Жуфтлик (r, s)
Бардошлилик	$\mu=1$ да даража параметри муаммо-сининг мураккаблигига асосланган (Афзаллиги DSA га нисбатан юқори бардошлилигида)	Модул 512-1024 бит бўлганда дискрет логари- фмлашининг мураккаблигига асосланган	Модул 255 битдан катта бўлганда ЭЭЧда дискрет логарифмлашининг мураккаблигига асосланган
Текириши калити шакли	Жуфтлик (y, z) $\mu=0$ да учлик (y, z, u_1) $\mu=1$ да (Афзаллиги сохта имзони аниқлашда)	Жуфтлик (g, y)	Параметр – Q
Имзо текириши натижаси шакли	Хэш-функция қиймати ёки хэшлашдан фойда- ланилмаганда хабар блоки (Афзаллиги хэшланиши шарт бўлмаган қисқа ха- барларни узатмаслик мумкинлиги)	Ижобий ёки салбий	Ижобий ёки салбий
Фойдалани- ладиган протокол	Стандартга хос ($\mu=1$ маромда камчилиги калитларни рўйхатга олиш марказига қўшимча юклама тушишида)	Анъанавий	Анъанавий
Фойдалани- ладиган маром	1. Сеанс калитисиз ($\mu=0$) 2. Сеанс калитили ($\mu=1$) (Афзаллиги янги имкониятлар тугилишида)	Сеанс калитисиз	Сеанс калитисиз
Биргаликдаги калитлар тури	R, R_1 параметрлар (Афзаллиги махфийлик даражасининг ортишида)	Йўқ	Йўқ
Сохта имзони аниқлаш калити тури	Жуфтлик (R_1, u_1) R_1 – назорат калити u_1 – сеанс ошкора калити (Афзаллиги)	Йўқ	Йўқ
Имзони тан олмаслик имконияти	Мавжуд (Афзаллиги)	Йўқ	Йўқ

Калитларни тақсимлаш пратокллари. Ушбу пратокллари истемолчи ва банк-эмитент ўртасида маълумот алмашилишида дастлабки қилинадиган иш саналаб, бунда икки томон ўртасида махфий маълумотларни

(асосан калитлар) алмашиниш амалга оширилади. Ушбу жараён ўтказилган тақдирда маълумотлар алмашиниш бошланади. Юбориладиган маълумотлар махфийлиги айнан шу жараёнда алмашинган калитларга боғлиқдир. Шуларни ҳисобга олган ҳолда қуйида калит тақсимлаш пратокллари таҳлили келтирилган [7].

11-жадвал

Симметрик алгоритмларидан фойдаланилган ҳолда калит алмашиниш пратокллари таҳлили

№	Протокол номи	A	B	K _A	K _B	K	t	S	Бўлиши мумкин бўлган ҳужум
1	Вақт меткасидан фойдаланиб калитни узатиш пратокли	+				+	-		Криптоаналитик бу маълумотни маълум вақтдан сўнг В фойдаланувчига қайта узатиши мумкин.
		-				+	+		В фойдаланувчи бу маълумотни ким томонидан узutilганини билмайди.
2	ЭРИ ёрдамидаги пратокл	+	+				+	-	В фойдаланувчи бу маълумотни ким томонидан узutilганини билмайди.
		+	+				-	+	Криптоаналитик бу маълумотни маълум вақтдан сўнг В фойдаланувчига қайта узатиши мумкин.
3	Тасодифий сонлардан фойдаланиб калитни генерация қилиш пратокли	+		-	-				Протокол бажарилиши натижасида сеанс калит генерация қилинмайди.
4	Диффи-Хелман пратокли	“Ўртадаги киши” ҳужумига бардошли эмас.							

12-жадвал

Ассиметрик алгоритмлардан фойдаланилган ҳолда калит алмашилиш
протоколлари таҳлили

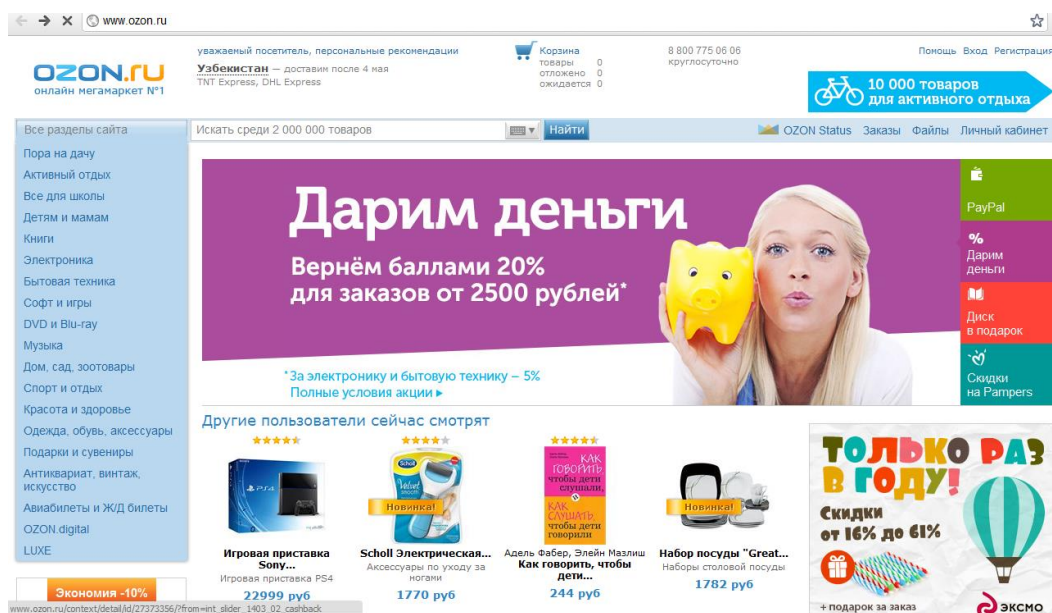
№	Протокол номи	A	B	r _A	r _B	r	t	Бўлиши мумкин бўлган ҳужум
1	Нидхем-Шредер протоколи	-	-	+				Арбитр маълумотни кимдан келгани ва кимга юбориш кераклиги ҳақида ҳеч нарса билмайди
		+	+	-		+		A фойдаланувчи маълумотни арбитрдан келганига тўла ишонч ҳосил қилолмайди
		-				+		B фойдаланувчи калитни ким томонидан юборилганини билмайди
		+				+		Криптоаналитик бу калитни маълум вақтдан сўнг қайта узутиши мумкин
2	Wide-Mouth Frog протоколи	+	+				-	Криптоаналитик бу маълумотни B фойдаланувчига такроран узатиши мумкин.
		-	-				+	Фойдаланувчилар маълумотнинг кимдан келганини билмайдилар.
3	Yahalom протоколи	+	+	-	-	+		Фойдаланувчилар ўртасида ўзаро идентификация таъминланмайди
4	Kerberos протоколи	Тизим вақтнинг синхрон равишда ишлаши талаб этилади.						

2. Интернет магазин тизимини яратиш

Интернет магазин интернет тармоғида электрон савдони амалга ошириш учун ишлаб чиқилган вертуал савдо дўконидир. Ушбу вертуал дўкон интернет тармоғида web-сайт кўринишида ишлаб чиқилади. Интернет магазин оддий web-сайтдан қуйидаги хусусиятлари бўйича фарқ қилади:

- Электрон тўлов тизимини мавжудлиги;
- Кенг ҳажмда товар ва хизматлар мавжудлиги;
- Товарни истемолчига этказиб бериш хизмати.

Қуйида Россиядаги биринчи рақамли Интернет магазин *ozon.ru* кўриниши келтирилган.



22-расм. ozon.ru Интернет магазини

Интернет магазиндан фойдаланиш тартиби қуйидагича:

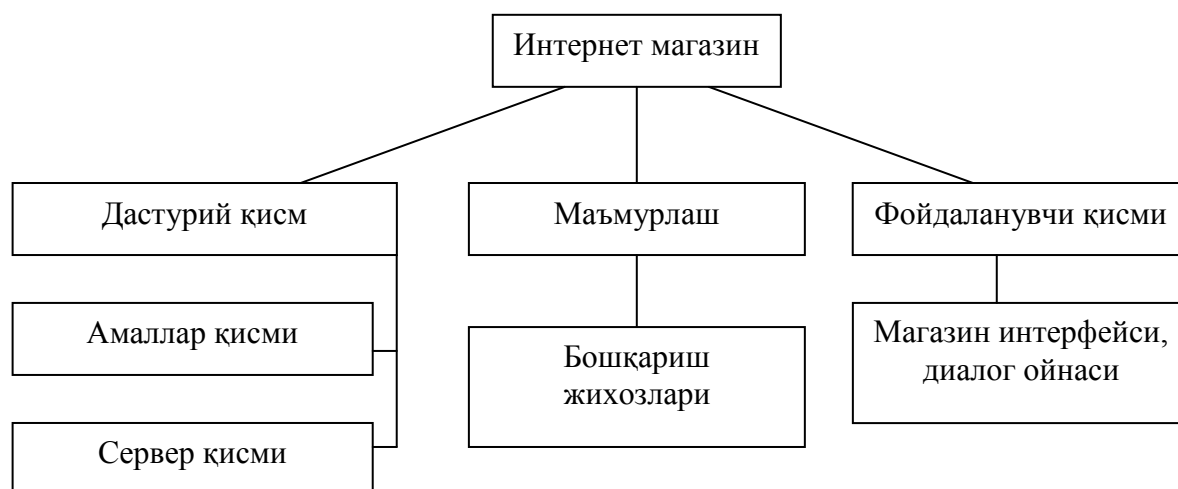
- Истемолчи виртуал магазиндан ўзига керакли товар ва хизмат турини танлайди, унинг хусусиятлари билан танишиб чиқади;
- Танланган товар ёки хизматдан фойдаланиш учун тўлов турини танлайди.
- Тўлов тури бўйича амалга оширилиб, истемолчига хабар юборилади.
- Сотиб олинган товар ёки хизмат истемолчига этказилади.

Интернет-магазин архитектураси содда қулай ва фойдаланишга осон бўлиши талаб этилиди ва у фойдаланувчи, дастурий ва маъмур қисмидан иборат(18-расм).

Дастурий қисм икки қисмдан ташкил топган бўлиб, улар амаллар қисми ва сервер қисми.

Амаллар қисмида Интернет-магазинни яратиш жихозлари ва воситалари қўрилади.

Сервер қисм яратилган Интернет магазинни сайт правайдерида жойлаштириш, қўлланилган технологиялардан иборат [7,8].



23-расм. Интернет-магазин архитектураси

Мўлжалланган Интернет-магазин php дастурлаш тили ёрдамида яратилган. Бундан ташқари Интернет-магазин тизимини яратишда ASP.NET, Perl ва Java дастурлаш тилларидан фойдаланилади.

Амалда онлайн тўловни амалга ошириш учун ушбу бўлимда дастурий воситалар ва компьютер техникасини сотувчи Интернет магазин ишлаб чиқилди (*UZITmagazine*).

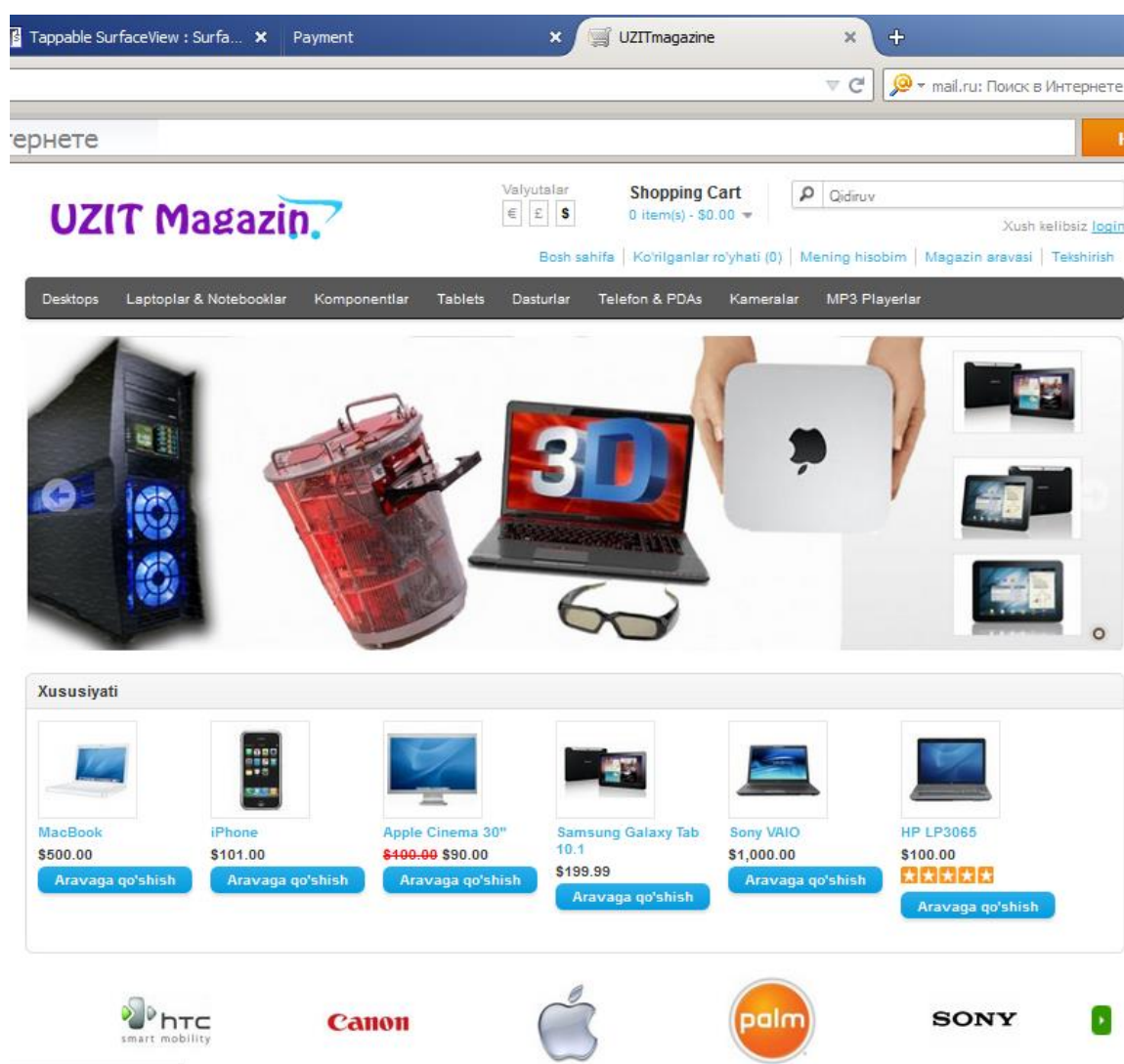
Ушбу Интернет магазинда фойдаланувчилар ўзларига керакли товарни ва тўлов турини танлашади. Тўлов усуллари эса 13-жадвалга келтирилган. Албатта ушбу тўлов барчаси амалга ошириш учун фойдаланувчига ушбу тўлов турини амалга ошириш учун рухсат ёки рўйхатдан утиш талаб этилади.

13-жадвал

Тизимда фойдаланилган тўлов турлари

Amazon Payments	Authorize.Net (AIM)	Bank Transfer	Cheque / Money Order
Cash On Delivery	Free Checkout	Klarna Account	Klarna Invoice

LIQPAY	Moneybookers	NOCHEX	Paymate
PayPoint	Payza	Perpetual Payments	PayPal Express Checkout
PayPal Payflow Pro iFrame	PayPal Website Payment Pro	PayPal Website Payment Pro iFrame	PayPal Payments Pro Payflow Edition
PayPal Payments Pro (UK)	PayPal Payments Standard	SagePay	SagePay Direct
Sage Payment Solutions (US)	2Checkout	Web Payment Software	WorldPay
Webmoney WME	Webmoney WMR	Webmoney WMU	Webmoney WMZ



25-расм. Интернет магазин кўриниши

3. Интернет-магазинда хавфсизликни таъминлаш

Ушбу қисмда Интернет магазинда хавфсизликни таъминлашнинг янги усуллари ва онлайн савдони амалга оширишда керакли тавфсиялар келтирилган[27].

Ҳозирги кунда мобиль воситасининг кенг тарқалганлиги ва электрон тижорат соҳасида ҳам кенг фойдаланилаётганлиги, ушбу тизимда ҳам хавфсизлик юзасидан қатор ишлар қилинишини белгилаб берди. Шундан келиб чиқиб қуйида ҳозирда фойдаланилаётган мобиль тўлов тизими ва янги тақдим этилган тўлов тизими келтирилган [14].



26-расм. Мобиль алоқа орқали тўлашнинг асос архитектураси

Хавфсиз тўлов транзакция тизимида эса тўлов қуйидагича амалга ошади.

Дастлаб истемолчи сотувчи веб саҳифасига ташриф буюради ва ўзига керакли хизмат ёки товарни танлайди. Товар ёки хизмат маълумотларини истемолси бирон бир компьютердан юборади. Масалан, товар нархи, телефон рақам ва ҳ.к. (аммо бирон бир молиявий амал бажарилмайди).

Сотувчи маълумотларни қабул қилиб олгач, истемолчига тасдиқлаш сўрови ва тўлов маълумотларни юборади. Шу эслатиб ўтиш керакки маълумотлар электрон рақамли имзо қўйилиб юборилади. Ушбу маълумотлар транзакция рақами, хизмат рақами, пул суммаси, сотувчи рақами ва банки рақами ва ҳ.к. Ушбу маълумотлар сотувчи маълумотлар базасида ҳам сақланади.

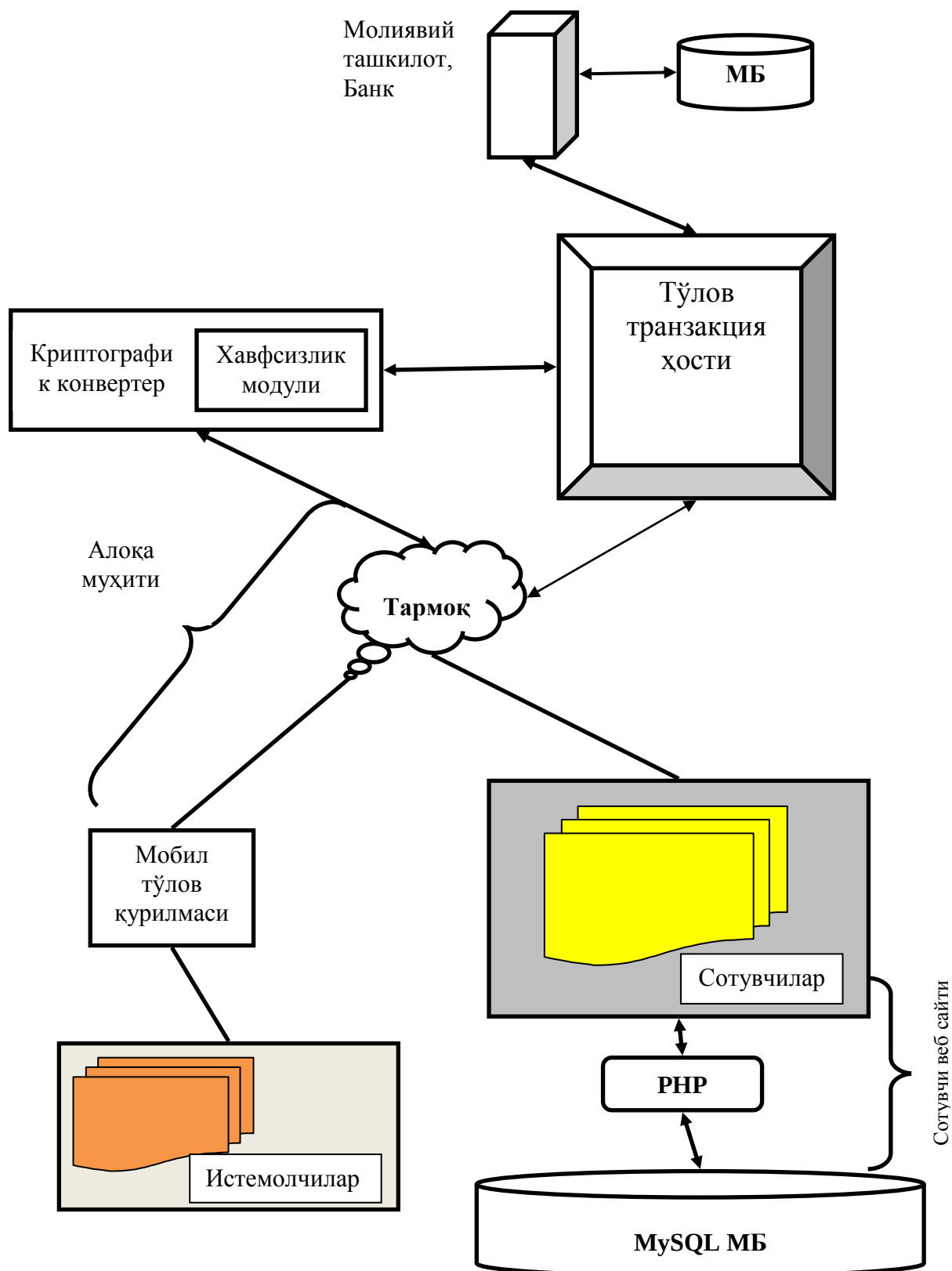
Олинган маълумотларни ва истемолчи маълумотларини биргаликда RSA очик калитли шифрлаш алгоритми ёрдамида очик калит билан шифрланади ва шифрланган маълумотлар эса криптографик конвертирга жўнатилади.

Криптографик конвертер олинган шифрланган матнни RSA нинг махфий калити билан дешифрланади. Очик матн қайтадан 3DES махфий калит криптографик тизим ёрдамида шифрланади ва транзакция ҳостида юборилади.

Тўлов жараёни. Дастлаб транзакция ҳости криптографик конвертир ҳостидан махфий калит билан шифрланган PIN олади.

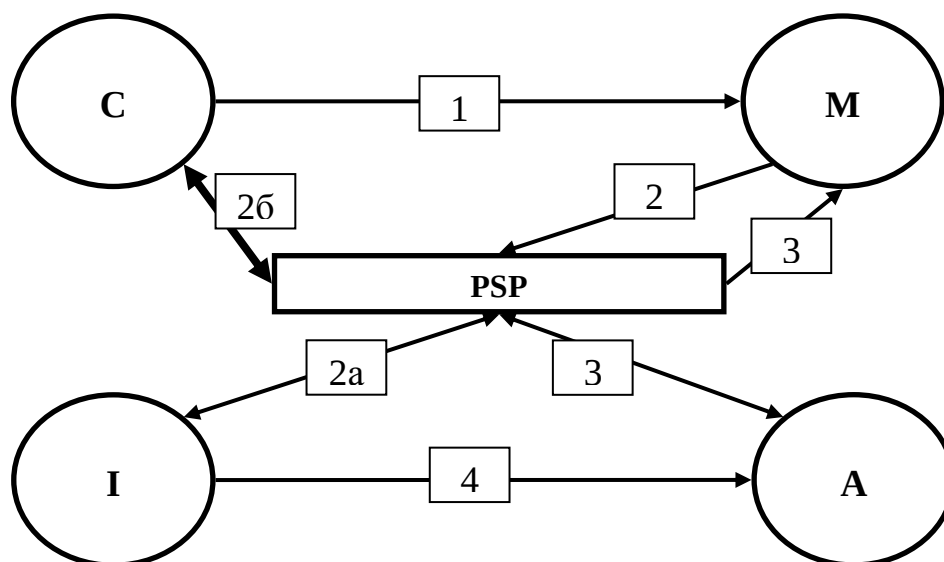
Шундан сўнг олинган шифрланган PIN ни транзакция ҳости махфий калит билан дешифрлайди. Бу ерда DES, 3DES, AES ёки Blowfish блокли шифрлаш алгоритмлари фойдаланилиши мумкин.

Транзакция ҳости дешифрланган матндан PIN кодни олади ва ушбу кодни текшириб кўради. Агар аутентификация мувофақиятли амалга оширилса, тўлов амалга оширилади. Акс ҳолда, транзакция қайтарилади [14].



27-расм. Хавфсиз тўлов транзакцияси тизими

Кенгайтирилган ананавий тўлов тизимига асосланган тўлов тизими. Ҳозирда мавжуд фойдаланилаётган тўлов тизими қуйидаги умумий архитектурага асосланади [16].

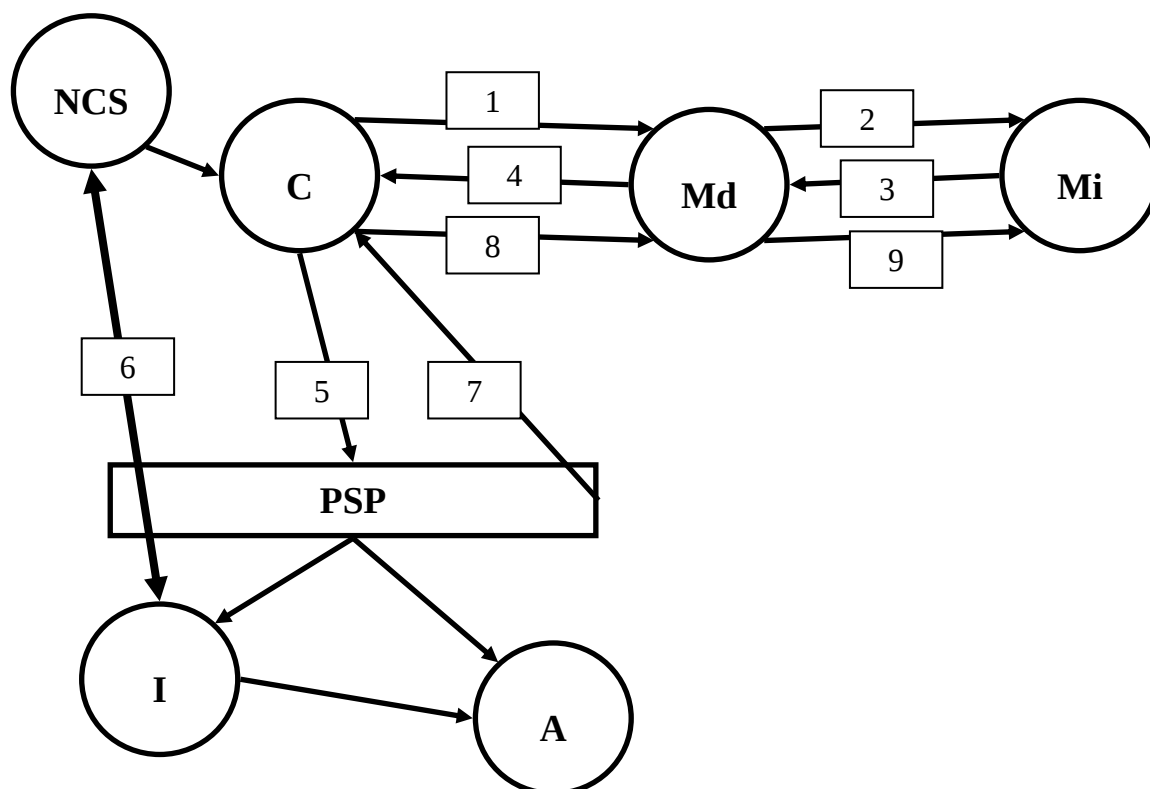


28-расм. Ананавий тўлов тизими

Бу ерда:

- C (Customer)-истмолчи;
- M(Merchant)-сотувчи;
- I(Issuer)- эмитент;
- A(Acquirer)-эквайер;
- PSP(Payment System Provider);
- 1. Тўлов маълумоти;
- 2. Авторизация сўрови;
- 2а. Авторизация сўрови;
- 2б. Аутертификация канали;
- 3. Авторизация жавоби;
- 4. Тўловни амалга ошириш.

Ушбу архитектурадан фойдаланган ҳолда ва янги технологик аспектлардан(тармоқ смарт картаси, бизнес воситачи) фойдаланган ҳолда куйидаги архитектурани кўриб ўтамиз.



29-расм. Кенгайтирилган ананавий тўлов тизимига асосланган тўлов

Бу ерда:

- C (Customer)-истмолчи;
- M(Merchant)-сотувчи;
- I(Issuer)- эмитент;
- A(Acquirer)-эквайер;
- Md(business mediator)-бизнес воситачи;
- Mi(Merchants)-сотувчилар;
- NSC(network smart card)-тармоқ смарт картаси;
- 1. Тўлов маълумоти;
- 2. Масофадаги сотувчига тўлов маълумоти юбориш;
- 3. Авторизация сўровини юбориш;
- 4. Авторизация сўровини юбориш;
- 5. Авторизация сўрови;
- 6. Аутентификация канали;
- 7. Авторизация натижаси;
- 8. Авторизация натижаси;

- 9. Авторизация натижаси.

Ушбу архитектурага асосан, истемолчи тўлов тизими правайдери ва бизнес воситачи орасида жойлашган. Ушбу архитектурада бизнес воситачи бир нечта сотувчиларни ягона истемолчи фойдаланиши учун боғлаб беради.

Ушбу ишлаб чиқилган архитектурада қуйидаги хавфсизлик талаблари қўйилади [13,14]:

1. Тармоқ смарт картаси учун:

- Масофадаги сервер ва смарт карта орасида ҳимояланган канал ҳосил бўлиши;
- Смарт карта ва эмитент банк орасида стандарт канал ва транспорт протоколи хавфсиз бўлиши шарт.

2. Бизнес воситачи:

- Хавфсизлик архитектураси жихатдан бизнес воситачини ишончли боғлаши керак;
- Тўлов маълумотини жўнатишда бизнес воситачини ишончли авторизация қилиш ва ҳар бир истемолчи орасида ишончли алоқани таъминлаш;
- Истемолчи билан сотувчи орасида ишонарли протокол орқали уланишни ва авторизацияни амалга ошириш;

3. Боғланишда:

- Барча жараёнларда юборилаётган маълумотлар ҳимояланган канал орқали амалга оширилиши шарт;
- Калит маълумотлар криптографик ҳимоя воситаларини қўллаган ҳолда юбориш.

4. Сотувчиларга:

- Савдони амалга ошириш жараёнида маълумотни тўлиқлигини, ўзгартирилмаганлигини текширувчи механизм мавжуд бўлиши;
- Савдо амалиётини ишончли саналган дастурий воситалар асосида амалга оширилиши;

- Савдо сайти, Интернет магазинни яратишда хавфсизлик нуқтаи-назаридан келиб ёндошув талаб этилади.

Керберос пратоколи асосида мобиль тўлов тизими. **Kerberos** протоколи **Нидхем-Шрёдер** протоколининг модификацион варианты ҳисобланади. А - фойдаланувчи В - фойдаланувчи билан маълумот алмашиши учун уларга сеанс калити қуйидагича амалга оширилади [7, 8]:

1. А - фойдаланувчи арбитрга ўзининг исми ва В - фойдаланувчининг исмидан ташкил топган маълумотни узатади:

$$A \rightarrow W: A, B$$

2. Арбитр иккита маълумотни ҳосил қилади, биринчиси вақт белгиси, ҳаётий вақт L, тасодифий сеанс калит ва А - фойдаланувчининг исмидан ташкил топган. Арбитр бу маълумотни ўзи ва В - фойдаланувчи учун умумий бўлган калит билан шифрлайди, иккинчиси вақт белгиси, ҳаётий вақт, тасодифий сеанс калит ва В - фойдаланувчининг исмидан ташкил топган. Арбитр бу маълумотни ўзи ва А -фойдаланувчи учун умумий бўлган калит билан шифрлайди. У иккала шифрматтни А -фойдаланувчига узатади:

$$W \rightarrow A: E_A(t, L, k, B), E_B(t, L, k, A) .$$

3. А - фойдаланувчи ўзининг калити билан биринчи шифрматтни дешифрлайди. У ўзининг исми ва вақт меткасини бирлаштириб, k - сеанс калит билан шифрлайди. Бу шифрматтни ва арбитрдан қабул қилган иккинчи шифрматтни В - фойдаланувчига узатади:

$$A \rightarrow B: E_k(A, t), E_B(t, L, k, A) .$$

4. В - фойдаланувчи ўзининг калити ёрдамида иккинчи шифрматтни дешифрлайди ва сеанс калитига эга бўлади. Бу сеанс калит ёрдамида биринчи шифрматтни дешифрлайди. Натижада ҳосил бўлган А - фойдаланувчининг исми ва вақт белгиси аввалгиси билан мос бўлса, В - фойдаланувчи А - фойдаланувчини идентификация қилади. Энди А - фойдаланувчи уни идентификация қилиши учун вақт белгисига 1 рақамини

кўшиб сеанс калит билан шифрлайди. Ҳосил бўлган шифрматнни А - фойдаланувчига узатади:

$$B \rightarrow A : E_k(t+1).$$

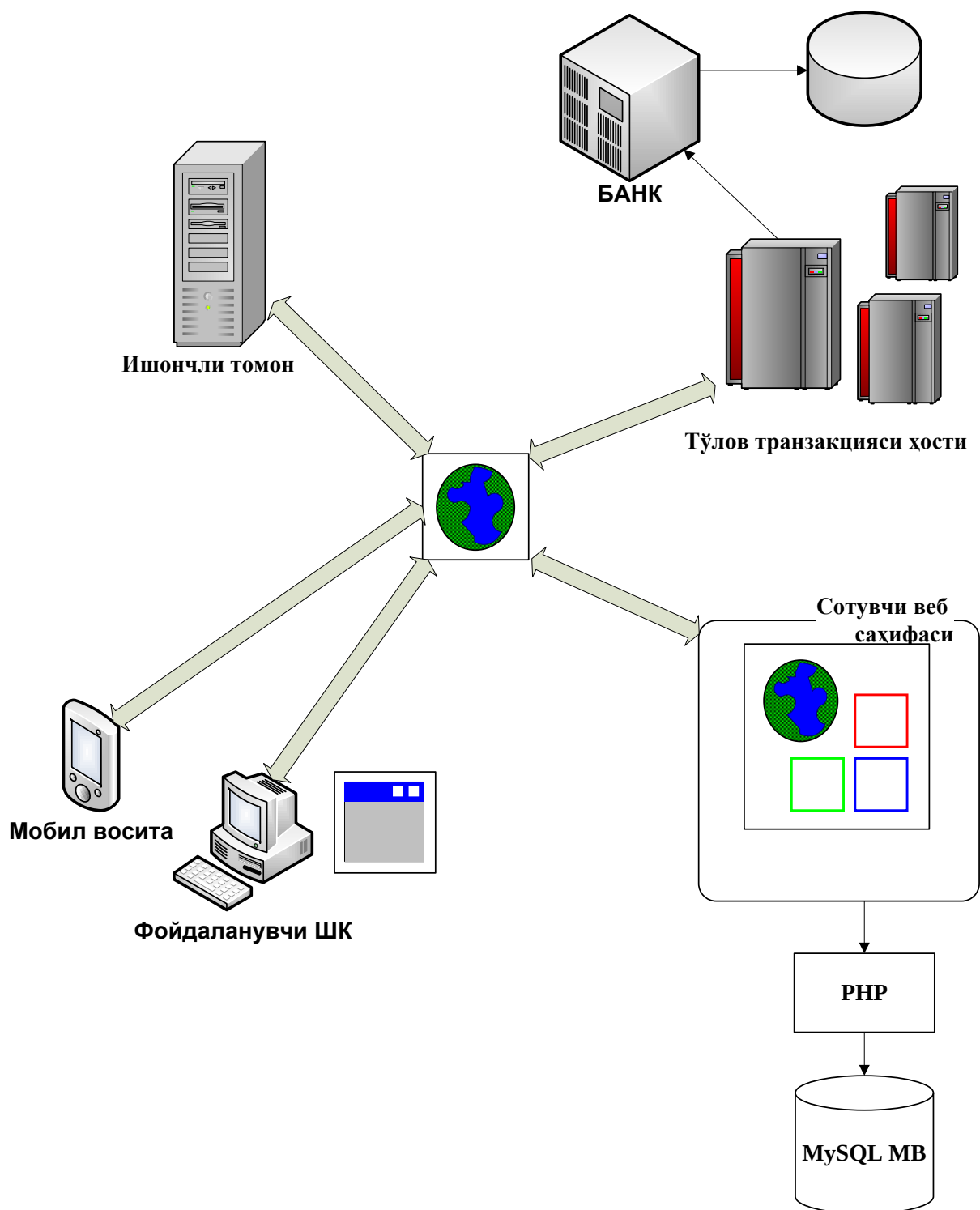
Агар ҳар бир фойдаланувчининг соатлари арбитрнинг соати билан синхрон равишда ишласа Бу протокол яхши натижа беради.

Ушбу пратоккол асосида мобиль восита ёрдамида тўловни амалга ошириш қуйидагича амалга оширилади. Ушбу ҳолатда шуни айтиб ўтиш керакки барча тармоқ SSL 3.0, TLS 1.0 ёки TLS 2.0 хавфсиз пратокколлари асосида амалга оширилади.

- 1. Харидор ва сотувчи алоқаси.** Истемолчи сотувчи веб сайти орқали ўзига керакли хизмат ёки товарни танлайди ва олди-сотди масаласига ойдинлик киритишади (нархи). Шундан сўнг харидор тўлов турини танлайди (мобиль алоқа воситаси ёрдамида тўлашни). Шундан сўнг сўров сотувчи серверига жўнатилади.

Мобиль алоқа воситаси. Мобиль алоқа воситаси махсус процессорга, хотирага ва дастурий воситалар эга. Шуни айтиб ўтиш керакки мобиль алоқа воситаси қўшимча пластик ёки кредит карта ўқувчи қурилмага эга[28].

Сотувчи томонидан келган тўлов маълумотлари истемолчи телефониға келиб тушади. Истемолчи телефони келган тўлов маълумотларини тўлдиради.



30-расм. Керберос пратоколи асосида мобил тўлов тизими

Юқорида келтирилган керберос пратоколи асосида тўлов транзакцияси хостини аутентификациядан ўтказади. Бунда у ишончли томондан фойдаланади. Тўлдирилган тўлов натижаларини, PIN кодни ва вақт параметрини сеанс калити ёрдамида шифрлаб жўнатади. Ушбу

жараёнда шифрлаш алгоритми сифатида AES ёки 3DES фойдаланиш тавсия этилади.

1. **Тўлов транзакция ҳости.** Тўловларни амалга ошириш маркази бўлиб, мобиль алоқа воситасидан келган сўровни текширади ва тўғри бўлса тўлов амалга оширилади. Агар натижа қониқарли бўлмаса тўлов рад этилиди.
2. Тўлов амалга оширилгач ҳар икки томонга тўлов ҳақидаги хабар жўнатилади.

Олинган натижалар эса қуйдагилар:

- Оддий PIN код асосида мобиль алоқа ёрдамида хавфсиз тўлов тизими ишлаб чиқилди;
- Фойдаланувчи юборадиган ва қабул қиладиган сўровлар SMS тарзида эмас Интернет тармоғи орқали узатилади;
- Тармоқдаги трафик криптобардошли саналган AES ёки 3DES асосида амалга оширилди;
- Аутентификациялашда эса криптобардошли саналган Керберос протоколидан фойдаланилди.

III боб бўйича хулосалар

- Электрон тўлов тизимларида фойдаланилаётган криптографик шифрлаш алгоритмлари, ЭРИ алгоритмлари, Хеш функциялар, очиқ калитли шифрлаш тизмлари ва аутентификациялаш протоколлари таҳлил этилди.
- Амалда онлайн тўловни жорий этиш мақсадида Интернет магазин тизими ишлаб чиқилди ва унда тўлов тизимлари уланди.
- SMS га асосланган мобиль алоқа воситасидан фойдаланган ҳолда амалга ошириладиган тўловлар ҳоўирги кунда заиф саналганлиги сабабли, янги PIN кодга асосланган мобиль алоқа тўлов тизими ишлаб чиқилди.

- Оддий тўловлардан фойдаланган ҳолда кенгайтирилган тўлов тизими таклиф этилди ва уларга хавфсизлик талаблари келтирилди.
- Керберес протоколига асосланган янги мобиль алоқа воситасида тўловни амалга ошириш тизими таклиф этилди. Бунда хавфсиз канал орқали PIN код асосида аутентификация амалга оширилди.

ХУЛОСА

Интернет тармоғининг ҳаётимизда кенг кириб келиши бир томондан кўплаб имкониятларни, масофадан туриб онлайн тўловни амалга ошириш орқали истемолчи хоҳишини ва истагини қондириш каби имкониятларни берса, бошқа томондан ушбу жараёнларда молиявий амаллар билан боғлиқ муаммоларни бартараф этиш масаласини келтириб чикаради. Ушбу муаммони замонавий ва бардошли саналган тизим билан ечиш эса ушбу магистрлик диссертациясининг асосий вазифасидир. Ушбу ишда қуйидаги натижалар олинди:

- Электрон тўлов тизимида мавжуд камчиликлар ва ҳозирги ҳолати таҳлил этилди;
- Электрон тўловни амалга ошириш воситалари ва усуллари таҳлил этилди. Уларнинг ютуқ ва камчиликлари айтиб ўтилди.
- Мобиль электрон тўлов тизимлари таҳлил этилди ва уларда хавфсизлик масаласи ўрганилди;
- Электрон тўловларни амалга оширишдаги ахборот хавфсизлигининг асоси саналган криптографик ҳимоя усуллари ва воситалари таҳлил этилди;
- Ҳозирда электрон тўлов тизими соҳасида йирик саналган корпорациялар, Visa ва MasterCard томонидан ишлаб чиқилган Visa 3-D Secure ва MasterCard SPA тўлов тизимлари ўзаро таҳлил этилди;
- Ананавий мобиль алоқа воситалари ёрдамида тўловни амалга ошириш усулини қараганда криптобардошли саналган янги усул таклиф этилди;
- Керберос пратоколига асосланган янги мобиль алоқа тўлов тизими таклиф этилди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Ўзбекистон Республикаси “Электрон тўловлар тўғрисида”ги Қонуни (16.12.2005 й., № ЎРҚ-13).
2. “Ахборотлаштириш тўғрисида”ги Ўзбекистон Республикаси қонуни, 11-декабр 2003-йил.
3. “Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари” тўғрисида Ўзбекистон Республикаси президентининг қарори.
4. “Миллий Ахборот-коммуникация тизимларининг компьютер хавфсизлигини таъминлаш борасидаги қўшимча чора-тадбирлар тўғрисида”ги Ўзбекистон Республикаси Президентининг қарори, 5 - сентабр 2005 – йил.
5. Ўзбекистон Республикаси “Электрон тижорат тўғрисида”ги қонуни. 2004 йил, 20 сон.
6. “Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш тўғрисидаги низомни тасдиқлаш ҳақида”ги Ўзбекистон Республикаси Вазирлар маҳкамасининг қарори, 21 - ноябр 2007 – йил.
7. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.
8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 -816 стр.
9. Практическая криптография. Нильс Фергюсон, Брюс Шнайер. 2005.
10. Visa 3-D Secure vs. MasterCard SPA. A comparison of online authentication standards. GPayments Pty Ltd. Pittwater Business Park Suite 8,5 Vuko Place Warriewood NSW 2102 Australia.
11. Verifed by Visa and MasterCard SecureCode: or, How Not to Design Authentication. Steven J. Murdoch and Ross Anderson. Computer

Laboratory, University of Cambridge, UK. Financial Cryptography and Data Security '10, 25-28 January 2010.

12. An Analysis and Comparison of Different Types of Electronic Payment Systems. Zon-Yau Lee, Hsiao-Cheng Yu, Pei-Jen Kuo. Institute of Management of Technology, Chiao-Tung University, Taiwan 30010 IBM Taiwan.
13. Recommendations for the Secerity of mobile payments. Draft document for public consulation. European central bank, Eurosystem. November, 2013.
14. Securing Mobile Payment Systems: Using Personal Identification Number (PIN) Method. Raphael Olufemi Akinyede, Olumide Sunday Adewale and Boniface Kayode Alese. Department of Computer Science, The Federal University. Proceedings of the International Conference on Software Engineering and Intelligent Systems July 5th-9th, Ota, Nigeria of Technology, Akure, Ondo-State, Nigeria. SEIS 2010 Vol 1.
15. Mobile Payments: Risk, Security and Assurance Issues. An ISACA Emerging Technology White Paper November 2011.
16. New E-Payment Scenarios in an Extended Version of the Traditional Model. Mildrey Carbonell, Joaquin Torres, Antonio Izquierdo, and Diego Suarez. Universidad Carlos III de Madrid Leganés (Madrid) Spain. 2008.
17. «Безопасность платежей в Интернете» Автор: И. Голдовский. Издательство: Питер; Серия: Электронная коммерция; 240 стр., 2006 г.
18. «Бизнес в Интернете. Финансы, маркетинг, планирование» Автор: Родион Костяев. Издательство: BHV - Санкт - Петербург, 2007 г.
19. «Как продать товар и получить деньги в Internet» (введение в электронную коммерцию) Автор: А. Крупник. Издательство: МикроАрт; 240 стр., 2004 г.
20. <http://click.uz/connect>
21. <http://smst.uz/>
22. <http://www.infinbank.com/en/retail/click>

23. http://en.wikipedia.org/wiki/Near_field_communication
24. http://en.wikipedia.org/wiki/Mobile_payment
25. http://en.wikipedia.org/wiki/Electronic_money
26. <https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/online-shopping>
27. Интернет магазин тизимида ахборот хавфсизлигини таъминлаш.
Алланов О.М. ЎзМУ хабарлари. 2014 й. 2 сон.
28. Электрон тижоратда химояланган тўловларни ташкил этиш.
Худойқулов З.Т., Алланов О.М.. Техника юлдузлари.