ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ХАЛҚ ТАЪЛИМИ ВАЗИРЛИГИ

САМАРҚАНД ВИЛОЯТИ ХАЛҚ ТАЪЛИМИ ХОДИМЛАРИНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ҲУДУДИЙ МАРКАЗИ

АХБОРОТЛАРНИ ҲИМОЯЛАШ ВА АНТИВИРУС ДАСТУРЛАРИДАН ФОЙДАЛАНИШ

(умумтаълим мактабларининг информатика ва ахборот технологиялари фани ўқитувчилари учун услубий кўрсатма)

Самарқанд – 2019

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ

ХАЛҚ ТАЪЛИМИ ВАЗИРЛИГИ

САМАРҚАНД ВИЛОЯТИ ХАЛҚ ТАЪЛИМИ ХОДИМЛАРИНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ҲУДУДИЙ МАРКАЗИ

АХБОРОТЛАРНИ ҲИМОЯЛАШ ВА АНТИВИРУС ДАСТУРЛАРИДАН ФОЙДАЛАНИШ

(умумтаълим мактабларининг информатика ва ахборот технологиялари фани ўқитувчилари учун услубий кўрсатма)

Самарқанд – 2019

Т.Кадиров– Ахборотларни ҳимоялаш ва антивирус дастурларидан фойдаланиш. Умумтаълим мактабларининг информатика ва ахборот технолигяилари фани ўқитувчилари учун услубий кўрсатма. - Самарқанд, 2019 й. 36 бет.

Масъул муҳаррир: **Б.Усманов –** СамВХТХҚТМОҲМ Аниқ ва табиий фанлар методикаси кафедраси мудири

Тақризчилар: **Э.Д.Умаров** – Муҳаммад Ал-Хоразмий номидаги ТАТУ Самарқанд Филиали “Ахборот технологиялари” кафедраси ўқитувчиси

Т.Ж.Оқназаров – СамВХТХҚТМОҲМ “Аниқ ва табиий фанлар методикаси” кафедраси ўқитувчиси

Услубий кўрсатма Аниқ ва табиий фанлар методикаси кафедрасининг 2019 йил 25 июньдаги 6-сонли йиғилиш қарори билан нашрга тавсия этилган.

СамВХТХҚТМОҲМ Илмий кенгашининг 2019-йил __июньда бўлиб ўтган йиғилишида муҳокама этилган ва __ сонли қарори билан нашрга тавсия этилган.

КИРИШ

“Таълим тўғрисида”ги қонун, “Кадрлар тайёрлаш миллий дастури”нинг амалиётга тўлиқ тадбиқ этилишини таъминлаш замонавий даражада билим, кўникма ва малакаларга эга бўлган бўлғуси мутахассисларни тайёрлашни талаб қилади.

Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегиясининг “Ижтимоий соҳани ривожлантириш” деб номланган тўртинчи йўналишда таълим ва фан соҳасини ривожлантириш, ёшларга оид давлат сиёсатини такомиллаштириш масалаларига алоҳида эътибор қаратилиб, мактабгача таълим муассасаларининг қулайлигини таъминлаш, умумий ўрта таълим, ўрта махсус ва олий таълим сифатини яхшилаш ҳамда уларни ривожлантириш чора-тадбирларини амалга оширишни назарда тутади. Шунингдек, таълим ва тарбия тизимининг барча бўғинлари фаолиятида бугунги замон талаблари асосида такомиллаштиришда тараққиёт стратегиямизнинг таълим соҳасидаги устувор йўналишлари таълим тизимини ривожланишининг янги босқичини белгилаб берди.

Таълим самарадорлигини ошириш, шахснинг таълим марказида бўлишининг ва ёшларнинг мустақил билим олишларини таъминлаш учун таълим муассасаларига яхши тайёргарлик кўрган ва ўз соҳасида билимларни мустаҳкам эгаллашдан ташқари замонавий педагогик технологияларни ва интерфаол усулларни, ахборот технологияларини қўллай оладиган тажрибали ўқитувчилар керак.

Ушбу услубий кўрсатма умумий ўрта таълим муассасаларида информатика ва ахборот технологиялари фанидан “Ахборотларни ҳимоялаш ва антивирус дастурларидан фойдаланиш” мавзусига эътибор қаратилган бўлиб, таълим муассасаларида ўқитаётган ва таҳсил олаётган ўқувчиларни компютер техникаси воситалари билан ишлаш жараёнида ахборотларни ҳимоялашга антивирус дастурларидан фойдаланиш масалаларига бағишланган.

Мазкур услубий қўрсатмада ахборотларни ҳимоялаш ва антивирус дастурларидан фойдаланишга эътибор қаратилган тавсиялардан ҳар бир ўқитувчи ўзи ўқитаётган фаннинг мазмуни, мақсади, шунингдек, мавжуд шароитлар ҳамда таълим олувчиларнинг имконияти ва эҳтиёжларидан келиб чиққан ҳолда фойдаланиши мумкин.

АХБОРОТ ХАВФСИЗЛИГИ ТУШУНЧАСИ

Ҳозирги кунда хавфсизликнинг бир қанча йўналишларини қайд этиш мумкин. Ахборотнинг мухимлик даражаси қадим замонлардан маълум. Шунинг учун ҳам қадимда ахборотни ҳимоялаш учун турли хил усуллар қўлланилган. Улардан бири - сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бошқа шахс ўқий олмаган. Асрлар давомида бу санъат - сирли ёзув жамиятнинг юқори табақалари, давлатнинг элчихона резиденсиялари ва разведка миссияларидан ташқарига чиқмаган. Фақат бир неча ўн йил олдин ҳамма нарса тубдан ўзгарди, яъни ахборот ўз қийматига эга бўлди ва кенг тарқаладиган маҳсулотга айланди. Уни эндиликда ишлаб чиқарадилар, сақлайдилар, узатишади, сотадилар ва сотиб оладилар. Булардан ташқари уни ўғирлайдилар, бузиб талқин этадилар ва сохталаштирадилар. Шундай қилиб, ахборотни ҳимоялаш зарурияти туғилади. Ахборотни қайта ишлаш саноатининг пайдо бўлиши ахборотни ҳимоялаш саноатининг пайдо бўлишига олиб келади.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Олдинги хавф фақатгина конфиденсиал (махфий) хабарлар ва хужжатларни ўғирлаш ёки нусха олишдан иборат бўлса, ҳозирги пайтдаги хавф эса компютер маълумотлари тўплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сўрамасдан фойдаланишдир. Булардан ташқари, бу харакатлардан моддий фойда олишга интилиш ҳам ривожланди.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатий регламентланган динамик технологик жараёнга айтилади.

Ахборотнинг эгасига, фойдаланувчисига ва бошқа шахсга зарар етказмокчи бўлган ноҳуқуқий муомаладан хар қандай хужжатлаштирилган**,** яъни идентификасия қилиш имконини берувчи реквизитлари қўйилган холда моддий жисмда қайд этилган **ахборот** ҳимояланиши керак.

Ахборот хавфсизлигини таъминлаш ва ахборот хавфсизлиги сиёсати даражасида ахборот хавфсизлиги нуктаи назаридан ахборотни қуйидагича туркумлаш мумкин:

• **махфийлик** — аниқ бир ахборотга факат тегишли шахслар доирасигина кириши мумкинлиги, яъни фойдаланилиши қонуний хужжатларга мувофик чеклаб қўйилиб, хужжатлаштирилганлиги кафолати. Бу банднинг бузилиши **ўғирлик** ёки **ахборотни ошкор қилиш,** дейилади;

• **конфиденсиаллик** — иншончлилиги, тарқатилиши мумкин эмаслиги,

махфийлиги кафолати;

• **яхлитлик** — ахборот бошланғич кўринишда эканлиги, яъни уни сақлаш ва узатишда рухсат этилмаган ўзгаришлар қилинмаганлиги кафолати; бу банднинг бузилиши **ахборотни сохталаштириш** дейилади;

• **аутентификасия** — ахборот захираси эгаси деб эълон қилинган шахс хақиқатан хам ахборотнинг эгаси эканлигига бериладиган кафолат; бу банднинг бузилиши **хабар муаллифини сохталаштириш** дейилади;

• **апеллясия қилишлик** — етарлича мураккаб категория, лекин электрон бизнесда кенг қўлланилади. Керак бўлганда хабарнинг муаллифи кимлигини исботлаш мумкинлиги кафолати.

Юкоридагидек, ахборот тизимига нисбатан қуйидагича таснифни келтириш мумкин:

• **ишончлилик** — тизим меёрий ва ғайри табиий холларда режалаштирилганидек ўзини тутишлик кафолати;

• **аниқлилик** — хамма буйруқларни аниқ ва тўлиқ бажариш кафолати;

• **тизимга киришни назорат қилиш** — турли шахс гурухлари ахборот манбаларига хар хил киришга эгалиги ва бундай киришга чеклашлар доим бажарилишлик кафолати;

• **назорат килиниши** — исталган пайтда дастур мажмуасининг хохлаган кисмини тулик текшириш мумкинлиги кафолати;

• **идентификасиялашни назорат қилиш** — хозир тизимга уланган мижоз аниқ ўзини ким деб атаган булса, аниқ ўша эканлигининг кафолати;

• қасддан **бузилишларга тўсқинлик** — олдиндан келишилган меъёрлар чегарасида қасддан хато киритилган маълумотларга нисбатан тизимнинг олдиндан келишилган холда ўзини тутиши.

Ахборотни ҳимоялашнинг мақсадлари куйидагилардан иборат:

- ахборотнинг келишувсиз чикиб кетиши, угирланиши, юкотилиши, узгартирилиши, сохталаштирилишларнинг олдини олиш;
- шахс, жамият, давлат хавфсизлилигига бўлган хавф - хатарнинг олдини олиш;
- ахборотни юк қилиш, ўзгартириш, сохталаштириш, нусха кучириш, тусиклаш бўйича рухсат этилмаган харакатларнинг олдини олиш;
- хужжатлаштирилган ахборотнинг микдори сифатида ҳуқуқий тартибини таъминловчи, ахборот захираси ва ахборот тизимига хар кандай ноқонуний аралашувларнинг куринишларининг олдини олиш;
- ахборот тизимида мавжуд бўлган шахсий маълумотларнинг шахсий махфийлигини ва конфиденсиаллигини сақловчи фуқароларнинг конституцион ҳуқуқларини ҳимоялаш;
- давлат сирини, қонунчиликка мос хужжатлаштирилган ахборотнинг

конфиденсиаллигини сақлаш;

- ахборот тизимлари, технологиялари ва уларни таъминловчи воситаларни яратиш, ишлаб чиқиш ва қўллашда субектларнинг ҳуқуқларини таъминлаш.

Ахборот ҳимояси - ахборот хавфсизлигини таъминлашга қаратилган тадбирлар, услублар ва воситалар мажмуасидан иборат. Шу билан бирга, ахборотни тўлалиги, компютер ашёлари ва унда сақланаётган дастурлар ҳамда маълумотларга рухсатсиз киришнинг олдини олиш, компютерлардаги дастурлардан рухсатсиз фойдаланишнинг олдини олиш каби вазифаларни бажаради.

Компютер тармоқларида ахборотни ҳимоялаш деб фойдаланувчиларни рухсатсиз тармоқ, элементлари ва заҳираларига эгалик қилишни ман этишдаги техник, дастурий ва криптографик усул ва воситалар, ҳамда ташкилий тадбирларга айтилади.

Ташкилий ҳимоялаш воситалари — бу талекоммуникасия ускуналарининг яратилиши ва қўлланиши жараёнида қабул қилинган ташкилий-техникавий ва ташкилий-ҳуқуқий тадбирлардир.

Ахлоқий ва одобий ҳимоялаш воситалари — бу ҳисоблаш техникасини ривожланиши оқибатида пайдо бўладиган тартиб ва келишувлардир. Ушбу тартиблар қонун даражасида бўлмасада, уни тан олмаслик фойдаланувчиларни обрўсига зиён етказиши мумкин.

Қонуний ҳимоялаш воситалари — бу давлат томонидан ишлаб чиқилган хуқуқий ҳужжатлар саналади. Улар бевосита ахборотлардан фойдаланиш, қайта ишлаш ва узатишни тартиблаштиради ва ушбу қоидаларни бузувчиларнинг масъулиятларини аниқлаб беради.

Ахборот хавфсизлигини таъминлаш. Ахборот хавфсизлигини таъминлаш - бу фойдаланувчининг ахборотларини ҳимоялашга қуйилган меъёр ва талабларни бажаришидир.

Ахборот хавфсизлигини таъминлаш муаммосига иккита ёндашув мавжуддир: “фрагментарй ва комплексли”.

«Фрагментарй ёндашув мавжуд шарт-шароитларда аниқ белгиланган таҳдидларга қарши акс таъсир кўрсатишга қаратилган. Бундай ёндашувни амалга оширишга мисол сифатида киришни бошқаришнинг айрим воситаларини, ихтисослашган антивирусли дастурларни келтириш мумкин.

Бундай ёндашувнинг афзал томони шундаки, бунда аниқ таҳдид бехато танлаб олинади. Унинг сезиларли камчилиги эса ахборотларга ишлов беришнинг ягона ҳимояланган муҳити йўқлигидадир.

Комплекс ёндашув Ахборот хавфсизлигида ахборотларга ишлов беришнинг ҳимояланган муҳитини яратишга қаратилган бўлиб, бу муҳит таҳдидларга қарши акс таъсирнинг турли хил чора-тадбирларини ягона комплексга бирлаштиради. Ахборотларга ишлов беришнинг ҳимояланган муҳитини ташкил этиш Ахборот хавфсизлигини маълум даражада кафолатлаш имконини беради, бу эса комплекс ёндашувнинг шубҳасиз афзаллигидан далолатдир. Бу ёндашувнинг камчиликлари қуйидагилардан иборат: Ахборот хавфсизлиги фойдаланувчиларининг ҳаракат эркинлиги чекланганлиги, ҳимоя воситаларини ўрнатиш ва созлашдаги хатоликларга юқори даражадаги сезгирлик, бошқаришнинг мураккаблиги.

Хавфсизлик сиёсати маъмурий-ташкилий чоралар, жисмоний ва дастурий-техник воситалар ёрдамида амалга оширилади ҳамда ҳимоя тизими архитекту-расини белгилаб беради. Ҳар бир муайян ташкилот учун хавфсизлик сиёсати махсус ишлаб чиқилиши ҳамда ундаги ахборот устида ишлашнинг аниқ техно-логияси ва қўлланаётган дастурий, техник воситаларга боғлиқ бўлиши керак.

Хавфсизлик сиёсати тизим обектларига мурожаат қилиш тартибини белги-лаб берувчи киришни бошқариш усули билан белгиланади. Хавфсизлик сиёсати-нинг иккита асосий тури фарқланади: **сайланма** ва **ваколатли.**

Сайланма хавфсизлик сиёсати мурожаатни бошқаришнинг танланадиган усулига асосланади. **Ваколатли хавфсизлик** сиёсати администратор томонидан тақдим этиладиган кўплаб рухсат этилган кириш муносабатларини билдиради. Одатда сайланма мурожаат бошқаруви хусусиятларини тавсиф этишда мурожаат матрисаси асосидаги математик моделдан фойдаланилади.

Кириш матрисаси бу шундай матрисаки, унда устун тизим обектига, сатр эса унинг субектига тўғри келади. Матрисанинг устун ва сатр кесишган жойида субектнинг обектга рухсат этилган мурожаат қилиш тури кўрсатилади. Одатда обектнинг субектга «қўйишга мурожаат», «ёзишга мурожаат», «ижрога мурожаат» ва ҳ.к. каби турлари қўлланади. Кириш матрицаси киришни бошқариш тизимларини моделлаштиришдаги энг содда ёндашув ҳисобланади. Бироқ у анча мураккаб моделлар учун асос вазифасини ҳам ўтайди.

Компютер тизимлари хавфсизлигини таъминлаш чоралари уларни амалга ошириш усуллари бўйича қуйидаги гуруҳларга бўлинади: ҳуқуқий (қонунчилик); ахлоқий-тарбиявий; маъмурий; жисмоний; техник-дастурий.

Санаб ўтилган ахборот хавфсизлиги чораларини ахборот ҳимояси йўлида кетма-кет қўйилган тўсиқ ёки чегаралар сифатида олиб қараш мумкин. Ҳимоя қилинаётган ахборотларга етиб бориш учун, кетма-кет бир нечта ҳимоя чегараларини босиб ўтиш лозим бўлади.

Ахборотларни ҳимоялашнинг техник ва дастурий воситалари Замонавий ахборот-коммуникация технологияларининг ютуқлари ҳимоя услубларининг бир қатор зарурий инструментал воситаларини яратиш имконини берди.

Ахборотларни ҳимояловчи инструментал воситалар деганда дастурлаш, дастурий-аппаратли ва аппаратли воситалар тушунилади. Уларнинг функсионал тўлдирилиши хавфсизлик хизматлари олдига қўйилган ахборотларни ҳимоялаш масалаларини ечишда самаралидир. Хозирги кунда тармоқ хавфсизлигини назорат қилиш техник воситаларининг жуда кенг спектри ишлаб чиқарилган.

Функционал вазифасига кўра ахборотларни муҳандис-техник ҳимоялаш воситалари қуйидаги гуруҳларга ажратилади:

Физик воситалар. **Бу воситаларга механик, электромеханик, электрон, электрон-оптик, радио ва радиотехник ва бошқа қурилмалар мансуб бўлади. Бу воситаларнинг вазифаси ахборотларга рухсатсиз киришни ва тажовузкорликни бошқа мумкин бўлган ҳаракатларни олдини олишдан иборат.**

Бу воситалар қуйидаги вазифаларни амалга ошириш учун қўлланилади:

• корхона ҳудудини қўриқлаш ва уни кузатиш учун;

• биноларни қўриқлаш ва уни назорат қилиш учун;

• жиҳозларни, маҳсулотларни, молиявий натижалар ва ахборотларни қўриқлаш учун;

• бино ва иншоатларни назорат қилувчи воситаларга киришни ҳимоя қилиш учун.

Барча обектларни ҳимоя қилишни физик воситаларини учта категорияга ажратиш мумкин:

огоҳлантириш воситалари (обект ўралган деворлар);

таҳдидни аниқлаш воситалари (сигнализация ва кузатиш учун ўрнатилган телевизорлари) ва **таҳдидни бартараф қилиш тизимлари** (ўт ўчириш воситалари).

Умуман олганда бу категорияларни қуйидаги гуруҳларга ажратиш мумкин:

• қўриқлаш ва қўриқлаш-ўт ўчириш тизимлари;

• қўриқлаш телевизорлари;

• қўриқлаш ёритгичлари;

• физик ҳимоялаш воситалари;

• аппарат воситалари.

Ахборотларни ҳимоялашни аппарат воситалари

Ахборотларни ҳимоялашни аппарат воситалари қуйидаги вазифаларни амалга оширишга имконият беради:

• ахборотни рухсатсиз чиқиб кетиш каналларини аниқлаш мақсадида техник воситаларни махсус текширувлардан ўтказиш;

• турли ҳил обектларни ахборотларни рухсатсиз чиқиб кетиш каналларини аниқлаш;

• ахборотни рухсатсиз чиқиб кетиши аниқланган каналларини локаллаштириш (ажратиб олиш);

• саноат шипионажи воситаларини қидириш ва аниқлаш;

• конфиденциал бўлган ахборотлар ва бошқа манбаларга рухсатсиз киришга қарши ҳаракатларнинг конфиденциал бўлиши.

Дастурий воситалар. Ахборотларни дастурий ҳимоялаш - бу ахборотларни ҳимоя қилиш вазифасини амалга оширувчи махсус дастурлар тизимидир. Конфиденсиал ахборотларнинг хавфсизлигини таъминловчи дастурлари қуйидаги йўналишларга ажратилиб кўрсатилади:

- ахборотларни рухсат берилмаган киришлардан ҳимоялаш;
- ахборотларни нусха олишдан ҳимоялаш;
- ахборотларни вируслардан ҳимоялаш;
- алоқа каналларини дастурий ҳимоялаш.

Ахборотларни рухсат берилмаган киришлардан ҳимоялашни дастурий воситаларини бажарадиган фимксиялари қуйидагилардан иборат бўлади:

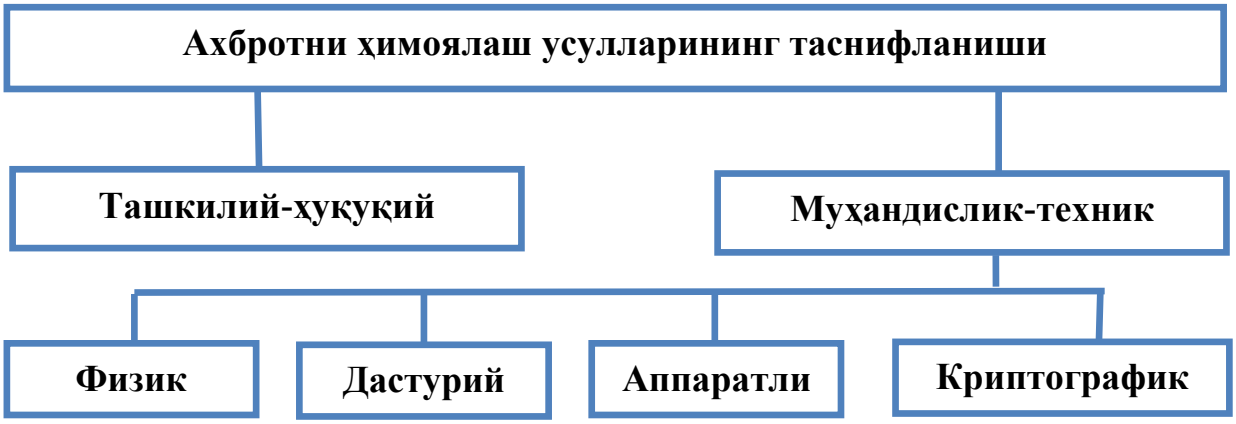
- обектлар ва субектлами идентификасиялаш;
- ҳисоблаш ресурслари ва ахборот ресурсларига киришга чекловлар ўрнатиш;

• ахборот ва дастурлар билан бўладиган ҳаракатларни назорат ва регистрасия қилиш.

Ахборотларни ҳимоялаш усуллари. Компютер тизимлари ва

тармоқларида ахборотни ҳимоя қилишнинг **ташкилий, ҳуқуқий** ва **техник усуллари** мавжуд.

Ахборотни ҳимоя қилишнинг ҳуқуқий усуллари, ихтиёрий вазифали ҳимоя қилиш тизимини расмий равишда кўриш ва ишлатишнинг асоси бўлиб хизмат қилади



Ташкилий усуллар бир нечта хавфларни бартараф этиш учун ишлатилса, **техник усуллар** ташкилий ва техник тадбирларга асосланган ҳолдаа кўпчилик ахборотларни ҳимоя қилади.

Ахборотни ҳимоя қилишнинг ҳуқуқий усуллари компьютер жиноятчилиги учун жазолаш меъёрларини ишлаб чиқиш.

Ахборотни ҳимоя қилишнинг ташкилий усуллари. Компьютер тизимларини қўриқлаш; ходимларни танлаб олиш; Ўта мухим ишларни фақат битта одам томонидан олиб борилиши ҳолатларини инкор қилиш; ишдан чиққандан кейин тизимни тиклаш режасининг мавжудлиги; ахборот хавфсизлиги тизимини таъминлайдиган шахсларга жавобгарликни бериш; компьютер марказини фрнатишга жой танлаш ва бошқалар.

Ахборотни ҳимоя қилишнинг техник усуллари аппаратли, дастурли ва аппарат-дастурлига бўлинади. Техник усулларда қуйидаги ҳарактердаги масалалар кўриб чиқилади: компютер тизимлари ва тармоқларида ахборотга рухсатсиз мурожаат қилишдан ҳимоя этиш; вирусдан ҳимоя қилиш; электромагнит, акустик майдон ва нурланишлар орқали «ушлаб» олишни бартараф этиш; криптографик усул асосида хабарларни юқори даражада ёпиқлигини инобатга олиш зарур.

Криптографик воситалар - тизим ва тармоқ бўйича узатиладиган, ЭҲМларда сақланадиган ва турли хил усуллар билан шифрланадиган ахборотларни ҳимоя қилишнинг махсус математик ва алгоритм воситаларидир.

Аутентикация, деганда субъект томонидан тақдим қилинган идентификаторни унга мансуб эканлигини текшириш ва унинг ҳақиқий эканлигини тасдиқлаш. Аутентикация - ахборот захираси ким эканлилигини ўрнатиш. Бошқача сўз билан айтганда аутентикация: ахборот ресурсларига кирмоқчи бўлган субъектнинг идентификаторини унга мансублигини текширишни ифодалайди.

Одатда аутентификация методлари қўлланиладиган воситаларига биноан синфланади. Бу холатда кўрсатилган методлар иккита гурухга ажратилади:

1. Тизим ресурсларига кириш хуцуцига, айрим сирли ахборотларга (парол) эга

бўлиш каби, шахснинг билимга асосланиш;

2. Жетон, электрон карта, пластик карта ва бошқа шу кабилар, киради.

Ахборотларни ҳимоялашда биринчи навбатда энг кенг қўлланилган дастурий воситалар ҳозирги кунда иккинчи даражали ҳимоя воситаси ҳисобланади. Бунга мисол сифатида парол тизимини келтириш мумкин.

Бевосита тармоқ бўйича узатиладиган маълумотларни ҳимоялаш мақсадида қуйидаги тадбирларни бажариш лозим бўлади: узатиладиган маълумотларни очиб ўқишдан сақланиш; узатиладиган маълумотларни таҳлил қилищдан сақланиш; узатиладиган маълумотларни ўзгартиришга йўл қўймаслик ва ўзгартиришга уринишларни аниқлаш; маълумотларни узатиш мақсадида қўлланиладиган дастурий узилишларни аниқлашга йўл қўймаслик; фирибгарлик йўли уланишларнинг олдини олиш.

Ушбу тадбирларни амалга оширишда асосан криптографик усуллар қўлланилади. Ахборотни ҳимоялаш учун **кодлаштириш** ва **криптография** усуллари қўлланилади.

Кодлаштириш деб ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади.

Криптография деб махфий хабар мазмунини шифрлаш, яъни малумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш йўли билан ахборотга рухсат этилмаган киришга тўсиқ қўйиш усулига айтилади.

Стенографиянинг криптографиядан бошқа ўзгача фарқи ҳам бор. Яъни унинг мақсади — махфий хабарнинг мавжудлигини яширишдир.

Ҳозирги вақтда ахборотни ҳимоялаш энг кўп қўлланилаётган соҳа бу — криптографик усуллардир. Криптография нуқтаи - назаридан шифр — бу калит демакдир ва очиқ маълумотлар тўпламини ёпиқ (шифрланган) маълумотларга ўзгартириш криптография ўзгартиришлар алгоритмлари мажмуаси ҳисобланади.

Калит — криптография ўзгартиришлар алгоритмининг баъзи-бир параметрларининг махфий ҳолати бўлиб, барча алгоритмлардан ягона вариантини танлайди. Калитларга нисбатан ишлатиладиган асосий кўрсаткич бўлиб **криптомустаҳкамлик** ҳисобланади. Криптография ҳимоясида шифрларга нисбатан қуйидаги талаблар қуйилади: етарли даражада криптомустахкамлик; шифрлаш ва қайтариш жараёнининг оддийлиги; ахборотларни шифрлаш оқибатида улар ҳажмининг ортиб кетмаслиги; шифрлашдаги кичик хатоларга тасирчан бўлмаслиги.

Ушбу талабларга қуйидаги тизимлар жавоб беради: ўринларини алмаштириш; алмаштириш; гаммалаштириш; аналитик ўзгартириш.

Ўринларини алмаштириш шифрлаш усули бўйича бошланғич матн белгиларининг матннинг маълум бир қисми доирасида махсус қоидалар ёрдамида ўринлари алмаштирилади.

Алмаштириш шифрлаш усули бўйича бошлангич матн белгилари фойдаланилаётган ёки бошқа бир алифбо белгиларига алмаштирилали.

Гаммалаштириш усули бўйича бошланғич матн белгилари шифрлаш гаммаси белгилари, яъни тасодифий белгилар кетма-кетлиги билан

бирлаштирилади.

Тахлилий ўзгартириш усули бўйича бошланғич матн белгилари аналитик формулалар ёрдамида ўзгартирилади, масалан, векторни матрисага кўпайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги бўлса, матриса эса калит сифатида хизмат қилади.

Ўринларни алмаштириш усуллари. Ушбу усул энг оддий ва энг кадимий усулдир. Ўринларни алмаштириш усулларига мисол сифатида қуйидагиларни келтириш мумкин: шифрловчи жадвал; сеҳрли квадрат. Шифрловчи жадвал усулида калит сифатида қуйидагилар қўлланилади: жадвал ўлчовлари; сўз ёки сўзлар кетма-кетлиги; жадвал таркиби хусусиятлари.

Ахборотни химоялашнинг мақсадлари куйидагилардан иборат:

- ахборотнинг келишувсиз чиқиб кетиши, ўғирланиши, йўқотилиши, ўзгартирилиши, сохталаштирилишларнинг олдини олиш;
- шахс, жамият, давлат хавфсизлилигига бўлган хавф-ҳатарнинг олдини олиш;
- ахборотни йўқ қилиш, ўзгартириш, сохталаштириш, нусха кўчириш, тўсиқлаш бўйича рухсат этилмаган ҳаракатларнинг олдини олиш;
- хужжатлаштирилган ахборотнинг миқдори сифатида хуқуқий тартибини таъминловчи, ахборот захираси ва ахборот тизимига ҳар қандай ноқонуний аралашувларнинг кўринишларининг олдини олиш;
- ахборот тизимида мавжуд бўлган шахсий маълумотларнинг шахсий махфийлигини ва конфиденциаллигини сақловчи фуқароларнинг конституцион хуқуқларини ҳимоялаш;
- давлат сирини, қонунчиликка мос ҳужжатлаштирилган ахборотнинг конфиденциаллигини сақлаш.

АХБОРОТ ХАВФСИЗЛИГИНИНГ ТАШКИЛИЙ-МАЪМУРИЙ ТАЪМИНОТИ

Ахборотни ишончли химоя механизмини яратишда ташкилий тадбирлар муҳим рол ўйнайди, чунки конфиденциал ахборотлардан рухсатсиз фойдаланиш асосан, техник жихатлар билан эмас, балки ҳимоянинг элементар коидаларини эътиборга олмайдиган фойдаланувчилар ва ходимларнинг жинояткорона харакатлари, бепарволиги, совукконлиги ва маъсулиятсизлиги билан боглик.

Ташкилий таъминот конфиденицал ахборотдан фойдаланишга имкон бермайдиган ёки жиддий кийинчилик туғдирувчи ижрочиларнинг ишлаб-чиқариш ва ўзаро муносабатларини меъёрий-ҳуқуқий асосида регламентлашдир.

Ташкилий тадбирларга қуйидагилар киради:

- хизматчи ва ишлаб чиқариш бино ва хоналарни лойихалашда, қуришда ва жихозлашда амалга ошириладиган тадбирлар. Бу тадбирларнинг асосий мақсади худудга ва хоналарга яширинча кириш имконини йўқотиш; одамларнинг ва транспортнинг юриши назоратининг қулайлигини таъминлаш; фойдаланишнинг алоҳида тизимига эга бўлган ишлаб-чиқариш зоналарини яратиш ва х.;

- ходимларни танлашда амалга ошириладиган тадбирлар. Бу тадбирларга ходимлар билан танишиш, конфиденциал ахборот билан ишлаш қоидалари билан ишлашни ўргатиш, ахборот ҳимояси қоидасини бузганлиги учун жавобгарлик даражаси ва бошқалар билан таништириш киради;

- ишончли пропуск режимини ва ташриф буюрувчиларнинг назоратини ташкил қилиш;

- хона ва ҳудудларни ишончли қўриқлаш;

- хужжатлар ва конфиденциал ахборот элтувчиларини сақлаш ва ишлатиш, шу жумладан қайд этиш, бериш, бажариш ва қайтариш тартибларига риоя қилиш;

- ахборот химоясини ташкил этиш, яъни муайян ишлаб чиқариш жамоаларида ахборот хавфсизлигига жавобгар шахсни тайинлаш, конфиденқиал ахборот билан ишловчи ходимлар ишини мунтазам текшириб туриш.

Бундай тадбирлар хар бир муайян ташкилот учун ўзига хос хусусиятга эга бўлади.

Ахборотни хужжатлаштириш қатъий белгиланган қоидалар ёрдамида амалга оширилади. Бу қоидаларнинг асосийлари ГОСТ 6.38-90 " Ташкилий-бошқарувчи хужжатлар тизими. Хужжатларни расмийлаштиришга талаблар", ГОСТ 6.10.4-84 "Унификақияланган хужжатлар тизими. Ҳисоблаш техника воситалари орқали яратилувчи машина элтувчиларидаги ва машинограммалардаги хужжатларга хуқуқий куч бериш" кабилар баён этилган. Бу ГОСТларда ахборотга хужжат хуқуқини берувчи 31 та реквизитлар кўзда тутилган, аммо бу реквизитларнинг барчасининг

хужжатда мавжудлиги шарт эмас. Асосий реквизит - матн. Шу сабабли, хар қандай равон баён этилган матн хужжат ҳисобланади ва унга хуқуқий куч бериш учун сана ва имзо каби мухим реквизитларнинг мавжудлиги кифоя.

Автоматлаштирилган ахборот тизимларидан олинган хужжатлар учун алохида тартиб қўлланилади. Бунда, маълум ҳолларда, масофадан олинган ахборот электрон имзо билан тасдиқланади. Ахборотни химоялаш учун барча ташкилий тадбирларни таъминловчи махсус маъмурий хизматни яратиш талаб қилинади. Унинг штат структураси, сони ва таркиби фирманинг реал эхтиёжлари, ахборотининг конфиденциаллик даражаси ва хавфсизлигининг умумий ҳолати орқали аниқланади. Маъмурий тадбирларга қуйидагилар киради:

- операцион тизимнинг тўғри конфигурациясини мададлаш;
- иш журналларининг назорати;
- пароллар алмашишининг назорати;
- ҳимоя тизимида "рахна"ларни аниқлаш;
- ахборотни ҳимояловчи воситаларни тестлаш.

Тармоқ операцион тизимининг тўғри конфигурациялашни одатда, тизим маъмури хал этади. Маъмур операцион тизим (одамлар эмас) риоя қилиши лозим бўлган маълум қоидаларни яратади. Тизимни маъмурлаш - конфигурация файлларини тўғри тузишдир. Бу файлларда (улар бир нечта бўлиши мумкин, масалан тизимнинг ҳар бир қисмига биттадан файл) тизим ишлаши қоидаларининг тавсифи бўлади.

Ҳавфсизлик маъмури компьютер тармоғи ҳолатини оператив тарзда (тармоқ компьютерлари ҳимояланиши ҳолатини кузатиш орқали) ва оператив бўлмаган тарзда (ахборот ҳимояси тизимидаги воқеаларни қайдловчи журналларни тахлиллаш орқали) назоратлаш лозим. Ишчи станциялар сонининг ошиши ва турли-туман компонентлари бўлган дастурий воситаларнинг ишлатилиши ахборот ҳимояси тизимидаги ходисаларни қайдлаш журналлар ҳажмини жиддий ошишига олиб келади. Журналлардаги маълумотлар ҳажми шунчалик ошиб кетиши мумкинки, маъмур улар таркибини жоиз вақт мобайнида таҳлиллай олмайди.

Тизим заифлигининг сабаби шундаки, биринчидан, фойдаланувчини аутентификациялаш тизими фойдаланувчи исмига ва унинг паролига (кўз тўридан фойдаланиш каби экзотик ҳолллар бундан мустасно), иккинчидан, фойдаланувчи тизимида тизимни маъмурлаш ҳуқуқи берилган супервизорнинг (supervisor) мавжудлигига асосланади. Супервизор паролини сақлаш режимининг бузилиши бутун тизимдан рухсатсиз фойдаланиш имконини яратади.

Ундан ташқари бундай қоидаларга асосланган тизим-статик, қотиб қолган тизим. У фақат қатъий маълум хужумларга қарши тура олиши мумкин. Олдиндан кўзда тутилмаган қандайдир янги тахдиднинг пайдо бўлишида тармоқ ҳужуми нафақат муваффақиятли, балки тизим учун кўринмайдиган бўлиши мумкин. Шунинг учун, муассасада ишлатилувчи ахборотнинг қайсиси ҳимояга мухтож эканлигини аниқ тасаввур қилиш муҳим ҳисобланади. Мавжуд ахборотни тахлиллашдан бошлаш лозим. Бу

муолажалар ахборот ҳимоясини таъминлаш бўйича тадбирларни дифференциаллаш имконини беради ва натижада, сарф-харажатларнинг қисқаришига сабаб бўлади.

Ахборот химояси тизимини эксплуатация қилиш боскичида хавфсизлик маъмурининг фаолияти фойдаланувчилар ваколатларини ўз вақтида ўзгартиришдан ҳамда тармоқ компьютерларидаги химоя механизмларини созлашдан иборат бўлади. Фойдаланувчилар ваколатларини ва компьютер тармоқларида ахборотни химоялаш тизимини созлашни бошқариш муаммоси, масалан, тармоқдан марказлаштирилган фойдаланиш тизимидан фойдаланиш асосида хал этилиши мумкин. Бундай тизимни амалга оширишда тармоқ асосий серверида ишловчи махсус фойдаланишни бошқарувчи сервердан фойдаланилади. Бу сервер марказий химоя маълумотлари базасини локал химоя маълумотлари базаси билан автоматик тарзда синхронлайди. Фойдаланишни бошқаришнинг бу тизимида фойдаланувчи ваколати вақти-вақти билан ўзгартирилади ва марказий химоя маълумотлари базасига киритилади, уларнинг муайян компьютерларда ўзгариши навбатдаги синхронлаш сеанси вақтида амалга оширилади.

Ундан ташқари фойдаланувчи паролини ишчи станцияларининг бирида ўзгартирса, унинг янги пароли марказий химоя маълумотлари базасида автоматик тарзда аксланади, ҳамда бу фойдаланувчи ишлашига рухсат берилган ишчи станцияларга узатилади.

КОМПЬЮТЕР ВИРУСЛАРИ, УЛАРНИНГ КЛАССИФИКАЦИЯСИ ВА УЛАР БИЛАН КУРАШИШ МЕХАНИЗМЛАРИ

Зараркунанда дастурлар ва аввало, вируслар компьютер тизимси учун жиддий хавф ҳисобланади. Бу хавфни назар писанд килмаслик фойдаланувчилар ахбороти учун жиддий оқибатларга сабаб бўлиши мумкин. Вирусларнинг хавфини хаддан ташқари ошириб юбориш ҳам компьютер тизимларининг барча имкониятларидан фойдаланишга салбий таъсир кўрсатади. Вируслар таъсири механизмини, улар билан курашиш методларини билиш вирусларга қарши самарали курашишни ташкил этишга, улар таъсири натижасида зарарланиш эхтимолини ва йўқотишларни минимумга келтиришга имкон беради.

«Компьютер вируси» атамаси 80-йилларнинг ўрталарида киритилган. Биологик вирусларга тегишли ўлчамларининг кичиклиги, ўз-ўзидан купайиб ва объектларга сингиб (уларни захарлаб) тез тарқалиш қобилияти, тизимга салбий таьсири каби аломатлар зараркунанда программаларга ҳам тааллуқлидир. Компьютер вируслари билан иш кўрилганда «вирус» атамаси билан бир қаторда «захарланиш», «яшаш мухити», «профилактика», каби тиббиёт атамаларидан хам фойдаланилади. «Компьютер вируслари» - компьютер тизимларида тарқалиш ва ўз-ўзидан қайтадан тикланиш (репликақия) хусусиятларига эга бўлган бажарилувчи ёки шархланувчи кичик программалардир. Вируслар компьютер тизимларида сақланувчи программа таьминотини ўзгартириши ёки йуқотиши мумкин.

Ҳозирда дунёда фақат руйхатга олинган 65 мингдан ортиқ компьютер вируслари мавжуд. Замонавий зараркунанда программаларининг аксарияти ўз-ўзидан кўпайиш қобилиятига эга бўлганликлари сабабли уларни ҳам компьютер вирусларига тааллуқли деб ҳисоблайдилар. Барча компьютер вируслари қуйидаги аломатлари бўйича классификацияланиши мумкин:

- яшаш мухити бўйича;
- яшаш мухитининг заҳарланиши бўйича;
- зараркунандалик таьсирнинг хавфи даражаси бўйича;
- ишлаш алгоритми бўйича.

Яшаш мухити бўйича компьютер вируслари қуйидагиларга бўлинади: тармоқ вируслари; файл вируслари; юклама вируслар; комбинацияланган вируслар.

Тармоқ вирусларнинг яшаш мухити компьютер тармоқларининг элементларидир. Файл вируслар бажарилувчи файлларда жойлашади. Файл вируслар ичида макровируслар алохида урин тутади. Макровируслар-макротилларда ёзилган зараркунанда прграммалар, электрон жадваллар ва х. Юклама вируслар ташқи хотира қурилмаларининг юклама секторларида (boot-секторларда) бўлади. Комбинацияланган вируслар бир неча яшаш мухитида жойлашган бўлади. Мисол тариқасида юклама файл вирусларни курсатиш мумкин.

Яшаш мухитининг заҳарланиши усули бўйича компьютер вируслари қуйидагиларга бўлинади:

• резидент;
• резидент бўлмаган.

Резидент вируслар фаоллашганларидан сўнг тўлалигича ёки қисман яшаш муҳитидан (тармоқ, юклама сектори, файл) ҳисоблаш машинасининг асосий хотирасига кўчади. Бу вируслар, одатда, фақат операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш мухитини захарлайди ва маьлум шароитларда зараркунандалик вазифасини бажаради.

Резидент бўлмаган вируслар фақат фаоллашган вақтларида ҳисоблаш машинасининг асосий хотирасига тушиб, захарлаш ва зараркунандалик вазифаларини бажаради. Кейин бу вируслар асосий хотирани бутунлай тарк этиб яшаш мухитида қолади. Агар вирус яшаш мухитини захарламайдиган программани асосий хотирага жойлаштирса бундай вирус резидент бўлмаган вирус деб ҳисобланади.

Вируснинг зараркунандалик имкониятлари уларни яратувчисининг мақсади ва малакасига ҳамда компьютер тизимларининг хусусиятларига боғлиқ.

Фойдаланувчининг информацион ресурслари учун хавф даражаси бўйича компьютер вирусларини қуйидагиларга ажратиш мумкин: безиён вируслар; хавфли вируслар; жуда хавфли вируслар.

Безиён компьютер вируслари компьютер тизими ресурсларига қандайдир шикаст етказишни ўзига мақсад қилмаган муаллифлар томонидан яратилади. Уларнинг мақсади, одатда, ўзларини дастурчининг имкониятларини кўз-кўз қилишдир. Бундай вирусларнинг зараркунандалиги моноторингда айбсиз матнларни ва расмларни, мусиқий парчаларнинг ижро этилишига олиб келади ва ҳ.

Аммо безарар бўлиб кўринган бундай вируслар компьютер тизимларига маьлум шикаст етказади. Биринчидан бундай вируслар компьютер тизимларини ресурсларини сарфлайди, натижада унинг ишлаш самарадорлиги пасаяди. Иккинчидан, компьютер вирусларида компьютер тизимларининг информацион ресурсларига шикаст келтирувчи хатоликлар бўлиши мумкин.

Хавфли вирусларга компьютер тизимларининг самарадорлигини жиддий пасайишига олиб келувчи, аммо хотирловчи қурилмаларда сақланувчи ахборотнинг яхлитлигини ва махфийлигини бузмайдиган вируслар киради. Бундай вируслар таъсири оқибатларини унчалик катта бўлмаган моддий ва вақтий ресурслар сарфи эвазига йўқотиш мумкин. Бундай вирусларга мисол тариқасида ҳисоблаш машинаси хотирасини эгалловчи, аммо тармоқ ишига таьсир қилмайдиган вирусларни, программани қайтадан ишланиш, операцион тизимининг қайтадан юкланиш ёки маълумотларни алоқа каналлари орқали қайтадан узатилиш ва х. заруриятини туғдирувчи вирусларни кўрсатиш мумкин.

Жуда хавфли вирусларга ахборотнинг махфийлигини бузилишига, йўқ қилинишига, қайтарилмайдиган турланишга (шифрлаш ҳам шу қаторда) ҳамда ахборотдан фойдаланишга тусқинлик қилувчи ва натижада аппарат

воситаларнинг ишдан чиқишига ва фойдаланувчилар соғлигига шикаст етишига сабаб бўлувчи вируслар киради.

Ишлаш алгоритмининг хусусиятлари бўйича вирусларни иккита синфга ажратиш мумкин.

тарқалишида яшаш маконини ўзгартирмайдиган тарқалишида яшаш маконини ўзгартирадиган.

Яшаш маконини ўзгартирмайдиган вируслар ўз навбатида иккита гурухга ажратилиши мумкин.

• вируслар-«йўлдошлар» (companion);

• вируслар-«қуртлар» (worm).

Вируслар-«йўлдошлар» файлларни ўзгартирмайди. Унинг таьсир механизми бажарилувчи файлларнинг нусхаларини яратишдан иборатдир.

Вируслар-«қуртлар» тармоқ орқали ишчи станцияга тушади, тармоқнинг бошқа абонентлари бўйича вирусни жўнатиш адресларини ҳисоблайди ва вирусни узатишни бажаради. Вирус файлларни ўзгартирмайди ва дискларнинг юклама секторларига ёзилмайди. Баьзи бир вируслар-«қуртлар» дискда вируснинг ишчи нусхасини яратади, бошқалари фақат ҳисоблаш машинасининг асосий хотирасида жойлашади.

Алгоритмларнинг мураккаблиги, мукаммалик даражаси ва яшириниш хусусиятлари бўйича яшаш маконини ўзгартирадиган вируслар қуйидагиларга бўлинади:

• талаба вируслар;

• «стелс» вируслар (кўринмайдиган вируслар);

• полиморф вируслар.

Талаба-вируслар малакаси паст яратувчилар томонидан яратилади. Бундай вируслар, одатда, резидент бўлмаган вируслар қаторига киради, уларда кўпинча хатоликлар мавжуд бўлади, осонгина танилади ва йўқотилади.

«Стелс» вируслар малакали мутахасислар томонидан яратилади. «Стелс»-вируслар операцион тизимнинг шикастланган файлларга мурожаатларини ушлаб қолиш йўли билан ўзини яшаш маконидалигини яширади ва операцион тизимни ахборотнинг шикастланмаган қисмига йўналтиради. Вирус резидент ҳисобланади, операцион тизим программалари остида яширинади, хотирада жойини ўзгартириши мумкин. «Стелс» - вируслар резидент антивирус воситаларига қарши таъсир кўрсата олиш қобилиятига эга.

Полиморф вируслар хам малакали мутахасислар томонидан яратилади, ва доимий танитувчи гурухлар-сигнатураларга эга булмайди. Оддий вируслар яшаш маконининг захарланганлигини аниқлаш учун захарланган объектга махсус танитувчи иккили кетма-кетликни ёки символлар кетма-кетлигини (сигнатурани) жойлаштиради. Бу кетма-кетлик файл ёки секторнинг захарланганлигини аниқлайди. Полиморф вируслар вирус танасини шифрлашдан ва шифрлаш программасини турлантиришдан фойдаланади. Бундай ўзгартириш эвазига полиморф вирусларда кодларнинг мувофиқлиги бўлмайди. Маълум вируслар билан ишлашда қулайликни

таъминлаш мақсадида вируслар каталогидан фойдаланилади. Каталогда вирусларнинг қуйидаги стандарт хусусиятлари тўғрисидаги маълумот жойлаштирилади: номи, узунлиги, захарланувчи файллар, файлдаги ўрни, захарлаш усули, резидент вируслар учун асосий хотирага жойлаштириш усули, келиб чиқарадиган натижалари, зараркунандалик вазифаларининг борлиги (йўқлиги) ва хатоликлар. Каталогларнинг мавжудлиги вирусларни тавсифлашда уларнинг стандарт хусусиятлари ва таъсирларини тушириб қолдириб, фақат ўзига хос хусусиятларини кўрсатишга имкон беради.

Вируслар билан курашиш методлари ва воситалари. Вируслар тарқалишининг оммалашуви, улар таъсири оқибатларининг жиддийлиги вирусга қарши махсус воситаларни ва уларни қўллаш методларини яратиш заруриятини туғдирди. Вирусга қарши воситалар ёрдамида қуйидаги масалалар ечилади:

1. Компьютер тизимларида вирусларни аниқлаш;
2. Вируслар таъсири оқибатларини йўқотиш.

Вирусларни аниқлашни уларнинг таъсири бошланиши биланоқ ёки, лоақал, зараркунандалик вазифалари бошланмасданоқ амалга ошириш мақсадга мувофиқ ҳисобланади. Таъкидлаш лозимки, барча хил вирусларнинг аниқланишини кафолатловчи вирусга қарши воситалар мавжуд эмас. Компъютер тизимларида вирусларни аниқлашнинг қуйидаги методлари мавжуд: сканерлаш, ўзгаришларни билиб қолиш, эвристик тахлил, резидент қоровуллардан фойдаланиш, дастурни вакцинациялаш, вируслардан аппарат-программ ҳимояланиш.

Сканерлаш - вирусларни аниқлашнинг энг оддий методларидан ҳисобланади. Сканерлаш программа-сканер томонидан амалга оширилади. Бу программа-сканер вирусларнинг танитувчи қисмини-сигнатурани қидириш мақсадида файлларни кўриб чиқади. Кўпинча программа-сканерлар аниқланган вирусларни йўқотиши мумкин. Бундай программалар полифаглар деб аталади. Сканерлаш усули сигнатуралари ажратилган ва доимий бўлган вирусларни аниқлашда қўлланилади.

Ўзгаришларни билиб қолиш усули программ-тафтишчидан фойдаланишга асосланган. Бундай программалар одатда вирус жойлашадиган дискнинг барча қисмлари характеристикаларини аниқлайди ва эслаб қолади. Программа-тафтишчининг даврий бажарилиши жараёнида сақланувчи характеристикалари билан диск қисмларини назоратлаш натижасидаги характеристикалар таққосланади. Тафтиш натижасида программа вируслар борлиги хусусида тахминга асосланган ахборотни беради.

Методнинг энг асосий афзаллиги - вирусларнинг барча хилини ҳамда номаълум вирусларни аниқлаши имкониятидир.

Эвристик тахлил усули ҳам ўзгаришларни билиб олиш методлари каби номаълум вирусларни аниқлаш имконини беради. Аммо бу метод файл тизими хусусидаги ахборотни олдиндан ёзиш, ишлаш ва сақлашни талаб этмайди. Эвристик тахлилнинг мохияти-вирусларнинг мумкин бўлган яшаш

маконларини текшириш ва улардаги вирусларга характерли командаларни (командалар гурухини) аниқлашдан иборатдир.

Резидент қоровулларидан фойдаланувчи усули ҳисоблаш машинасининг асосий хотирасида доимо сақланувчи ва бошқа программалар харакатини кузатувчи программаларга асосланган. Бу методнинг, жиддий камчилиги сифатида ёлғон-дакам тревогалар фоизининг кўплигидир.

Дастурни вакцинациялаш деганда унинг яхлитлигини назорат қилиш мақсадида махсус модулнинг яратилиши тушунилади. Файл яхлитлигининг характеристикаси сифатида одатда назорат йиғиндисидан фойдаланилади. Вакцинацияланган файлнинг захарланиши содир бўлса назорат модули назорат йиғиндисининг ўзгаришини аниқлайди ва бу хусусида фойдаланувчини огохлантиради.

Вирусларга қарши аппарат-программ воситалардан фойдаланиш усули вируслардан химояланишнинг энг ишончли усули ҳисобланади. Ҳозирда шахсий компьютерларни химоялашда махсус контроллерлар ва уларнинг программ таъминотидан фойдаланилади. Контроллер умумий шинадан фойдалана олади ва шу сабабли диск тизимига бўлган барча мурожаатларни назорат қила олади. Контроллернинг программ таъминотида ишлашнинг оддий режимида дискнинг ўзгартирилиши мумкин бўлмаган қисмлари хотирланади. Вирусларга қарши аппарат-программ воситалар қуйидаги афзалликларга эга: доимо ишлайди; таъсир механизмидан қатъий назар барча вирусларни аниқлайди; вирус таъсири ёки малакасиз фойдаланувчи иши натижасидаги рухсатсиз харакатларни тўхтатади. Бу воситаларнинг камчилиги сифатида уларнинг шахсий компьютер аппарат воситаларига боғлиқлигини кўрсатиш мумкин.

Вируслар таъсири оқибатларини йўқотиш жараёнида вирусларни йўқотиш ҳамда вирус бўлган файллар ва хотира қисмларини тиклаш амалга оширилади. Вирусларга қарши программлар ёрдамида вируслар таъсири оқибатларини йўқотишнинг икки усули мавжуд.

Биринчи методга биноан тизим маълум вируслар таъсиридан сўнг тикланади. Вирусни йўқотувчи программани яратувчи вируснинг стуктурасини ва унинг яшаш маконида жойлашиш характеристкаларини билиши шарт.

Иккинчи метод номаълум вируслар билан захарланган файлларни ва юклама секторини тиклашга имкон беради. Файлларни тиклаш учун тикловчи программа файллар хусусидаги вируслар йўқлигидаги ахборотни олдиндан сақлаши лозим. Захарланмаган файл хусусидаги ахборот ва вируслар ишлашининг умумий принциплари хусусидаги ахборотлар файлларни тиклашга имкон беради.

Антивирусларнинг вазифасига кўра турлари. Ҳозирги вақтда вирусларни йўқотиш учун кўпгина усуллар ишлаб чиқилган ва бу усуллар билан ишлайдиган дастурларни **антивируслар** деб аташади.

Антивирусларни, қўлланиш усулига кўра, қуйидагиларга ажратишимиз мумкин: ***детекторлар, фаглар, вакциналар, прививкалар, ревизорлар.***

Детекторлар — вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича тезкор хотира ва файлларни кўриш натижасида маълум вирусларни топади ва хабар беради. Янги вирусларни аниқлаб олмаслиги детекторларнинг камчилиги ҳисобланади.

Фаглар — ёки докторлар, детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги ҳолатига қайтаради (**Касперскй Антивирус, Нортон АнтиВирус, Доктор Веб, Панда, нод32**).

Вакциналар — юқоридагилардан фарқли равишда ҳимояланаётган дастурга ўрнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан вақтинча қилиниши унинг камчилиги ҳисобланади. Шу боис ҳам, ушбу антивирус дастурлари кенг тарқалмаган (**Anti Trojan Elite, Trojan Remover, Dr.Web CureIt**).

Прививка — файлларда ҳудди вирус зарарлангандек из қолдиради. Бунинг натижасида вируслар «прививка қилинган» файлга ёпишмайди. Вируслар зарарланган файлларга метка қўяди ва кейинги сафар бу файлни зарарламайди, прививка антивируслари эса олдиндан зарарланган деган метка қўйиб қўяди ва шу орқали файлни зарарлашдан сақлайди.

Филтрлар — қўриқловчи дастурлар кўринишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақда фойдаланувчига хабар беради (**Outpost Security Suite, Agnitum Outpost Firewall**). Филтр дастурлар компютер ишлаш жараёнида вирусларга хос бўлган шубҳали ҳаракатларни топиш учун ишлатилади.

Бу ҳаракатлар қуйидагича бўлиши мумкин:

• файллар атрибутларининг ўзгариши;

• дискларга доимий манзилларда маълумотларни ёзиш;

• дискнинг ишга юкловчи секторларига маълумотларни ёзиб юбориш.

Ревизорлар (CRC-skaner, Monitor) — энг ишончли ҳимояловчи восита бўлиб, дискнинг биринчи ҳолатини хотирасида сақлаб, ундаги кейинги ўзгаришларни доимий равишда назорат қилиб боради (**Kaspersky Monitor**).

Янги вирусларнинг тўхтовсиз пайдо бўлиб туришини ҳисобга олиб, антивирус базаларини доимий равишда янгилаб туриш лозим, ундан ташқари антивирус дастурларини янги версияларини чиқишини ҳам кузатиб бориш керак ва компютер (процессор, оператив хотира, операцион тизим) га мос келадиганларини аниқлаб дастурни янгилаб бориш шарт.

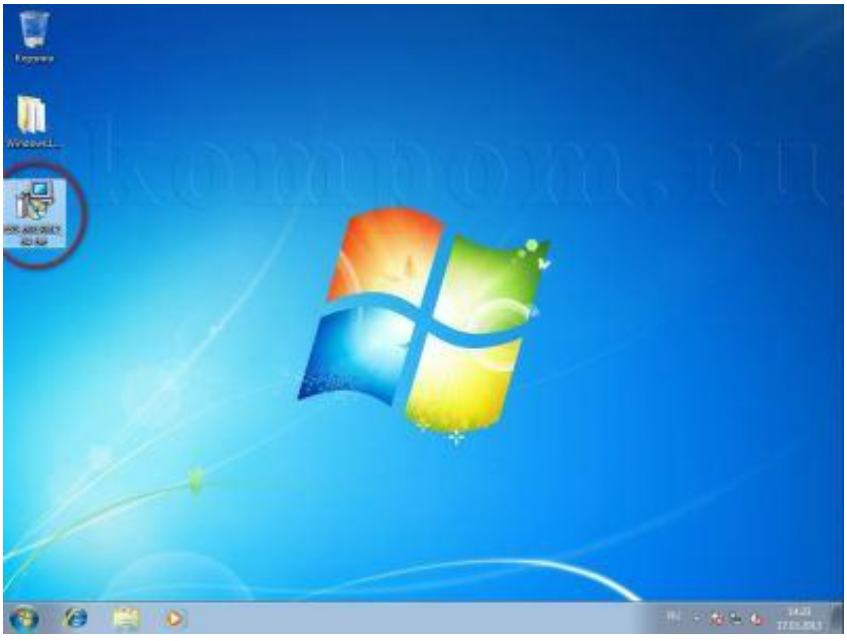
АНТИВИРУС ESET NOD32: ЎРНАТИШ, ЎЧИРИШ, ДАСТЛАБКИ СОЗЛАШ

Ҳозирги вақтда Kasperskiy, Dr.Web, Avast, Avira, Norton antivirus, Panda, ESET NOD32 ва бошқалар кўплаб антивирус дастурлари мавжуд. Кўпчилиги мураккаб антивирус деб қараладиган ушбу антивирус дастурларининг оммабоплиги уларнинг эркин фойдаланишлари билан қўлга киритилди. Аслида, бу ўзбошимчалик билан.

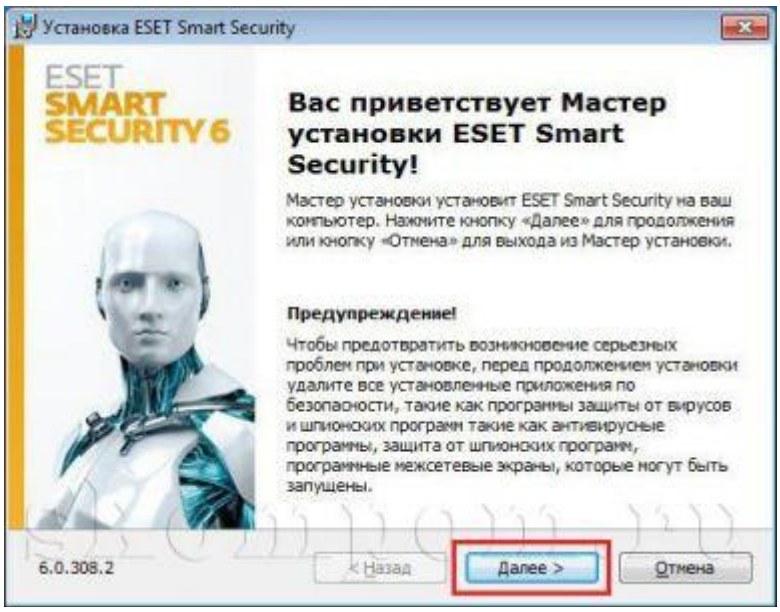
Антивирус дастурий таъминотидан фойдаланган ҳолда пулни тежаш, бизни доимий равишда барча турдаги бепул фойдаланишни қидирадиган "кулибин" маълумотларини олишга ёрдам беради. Ҳар бир оддий фойдаланувчи антивирус ва бошқа дастурлар учун ҳақ тўланадиган лицензияни харид қила олмайди. Ва агар ҳар бир киши камида 15-20 асосий дастурни қўллаганини ҳисобга олсангиз, унда сиз қанақа тирноқ бўлиши мумкинлигини тасаввур қилишингиз мумкин.

Юқорида санаб ўтилган антивирусларнинг барчасини бир мунча даражада ишлатилади. Антивирус NOD32 64 битли хавфсизлик девори билан бирга номланди ESET Smart Хавфсизлик 64-бит ёки қисқа ESS 64-бит. Сизнинг маълумотларингиз ва компютер компонентларини ўзлари ҳимоя қилиш учун ўрнатишни таклиф қиладиган нарса.

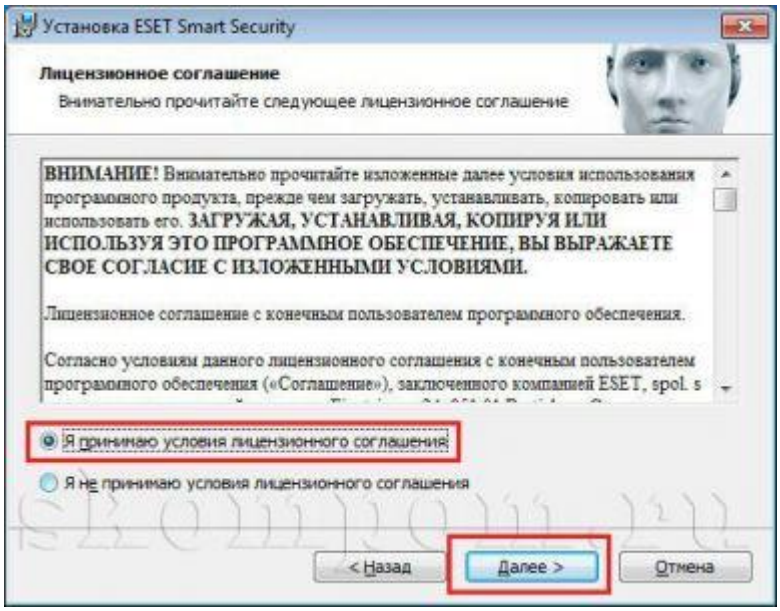
Ўрнатиш файлини компютерга юклаш билан ҳеч қандай муаммо туғилмаган деб тахмин қиламиз. Шундай қилиб, ESS_6.0.308.2_64-бит.мси файлини чап сичқонча билан икки марта босиш билан бошлаймиз.



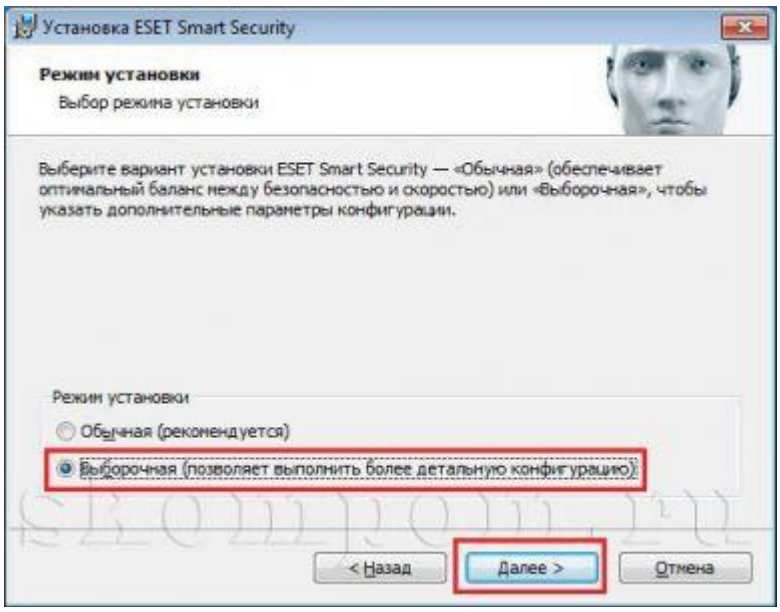
Антивирус дастурининг илгари ўрнатилган версияларини ўчиришни тавсия этувчи огоҳлантириш ойнаси ўрнатилган ўрнатиш устаси ишга тушади. Антивирус дастури ўрнатилган бўлса, уни ўчиринг ва "Кейинги" тугмасини босиб ESS ни ўрнатишни давом этамиз. Айни пайтда, пастки чап бурчакда ўрнатилган антивирус версиясини кўришингиз мумкин.



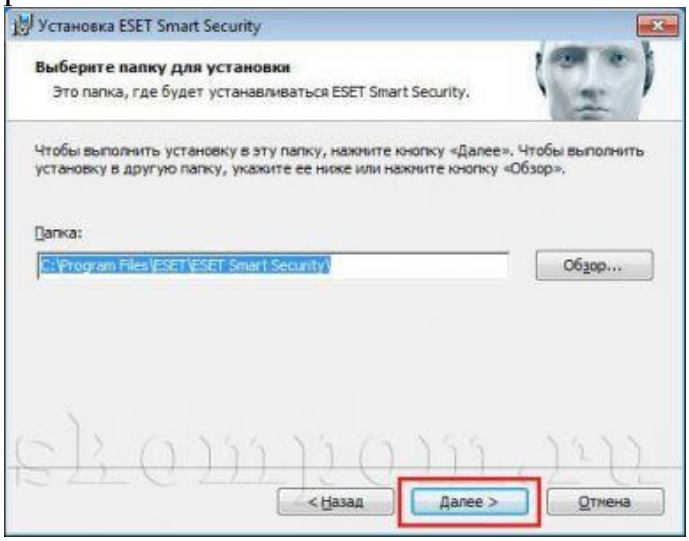
Шундан кейин лицензия шартномасига эга бўлган ойна пайдо бўлади. Агар ESS антивирусидан фойдаланиш шартлари қониқарли бўлса, "Мен лицензия шартномасининг шартларини қабул қиламан" ни танлаб, “Далее” ёки "Кейинги" тугмасини босамиз.



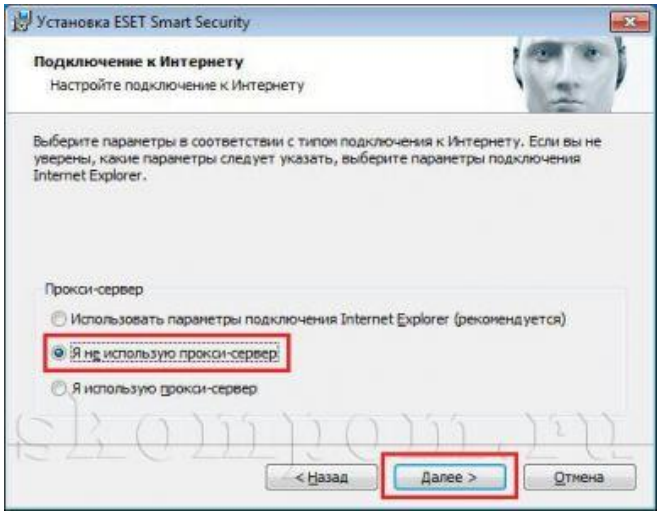
Тизим бизга иккита ўрнатиш режимини тақдим этади: нормал (ёки одатий) ва одатий. Махсус режимни танлашни таклиф қиламан ва “Далее” ёки "Кейинги" тугмасини босамиз.



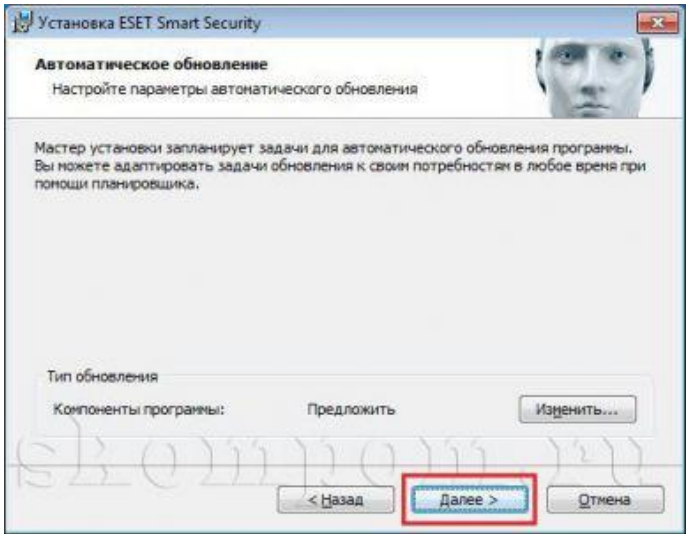
Кейинги ойнада биз ESET антивирусини ўрнатадиган папкани танлашимиз мумкин Smart Securitiy 6. Одатда стандарт папкадан кетаман. Биз "Кейинги" га борамиз.



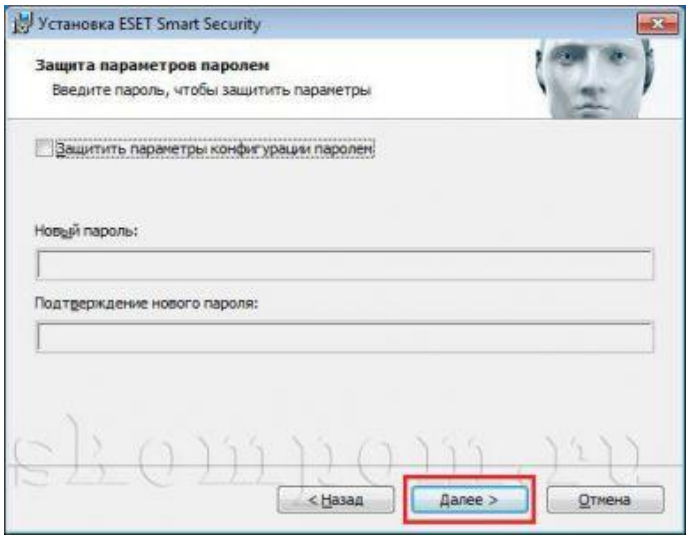
Энди Интернетга уланиш турини танлашингиз сўралади. Аксарият фойдаланувчилар прокси-серверсиз интернетга уланиш имконига эга. Биз ушбу элементни танладик, сўнгра "Кейинги" тугмасини босамиз.



Созланадиган ойналар пайдо бўлади. автоматик янгиланишлар антивирус ESS. Стандарт созламалардан мамнунман, чунки янгиланиш менинг розилигимдан кейин амалга оширилади. "Кейинги" тугмасини босамиз.

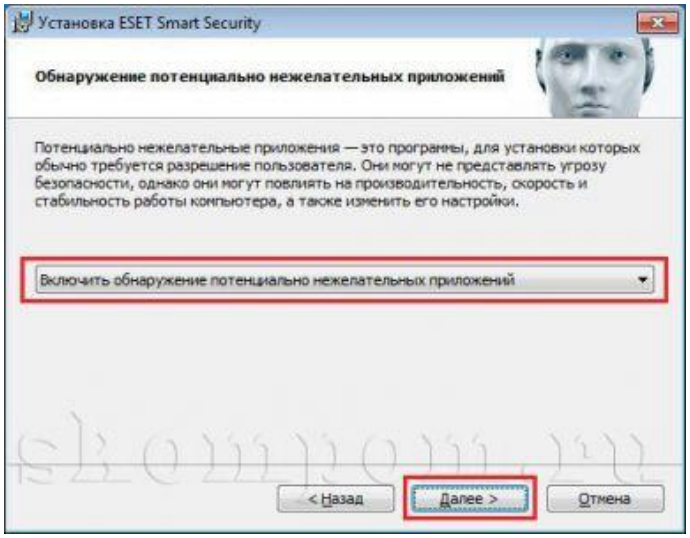


Ўрнатиш тизими антивирус конфигурацияси параметрларини парол билан ҳимоя қилишни таклиф қилади. Агар сиз паролни ўрнатган бўлсангиз, антивирус дастурининг созламаларидан фойдаланиш фақат уни биладиган кишига мумкин бўлади. Биз одатда паролсиз қолдирамиз. Биз "Кейинги" га борамиз.

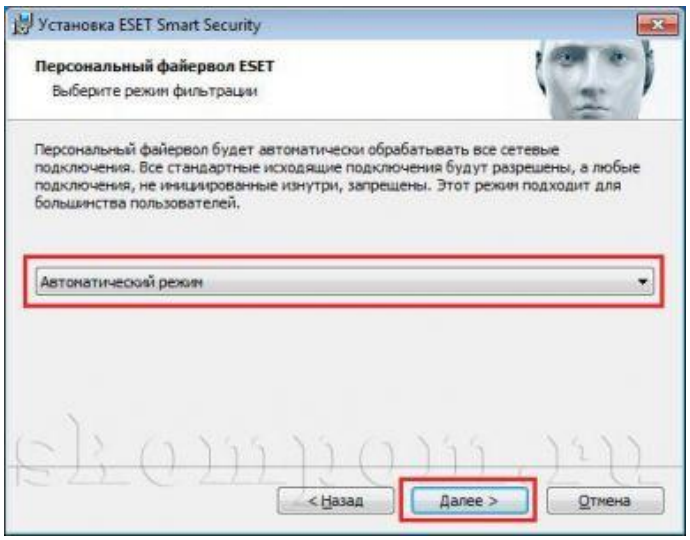


Кейинги қадам ESET Ливе Грид хизматини ёқиш ёки ўчириш, бу сизнинг компютерингизни қўшимча равишда ҳимоя қилишга имкон беради. Буни миллионлаб бошқа ESS фойдаланувчилари, шу жумладан сиз тақдим этган маълумотлар асосида амалга оширади. Одатда уни тарк этамиз. Лекин ташвиш қилишингиз керак эмас, дастурнинг илғор параметрлари ўрнатилгандан сўнг уни ёқишингиз ва ўчиришингиз мумкин. "Кейинги" тугмасини босамиз.

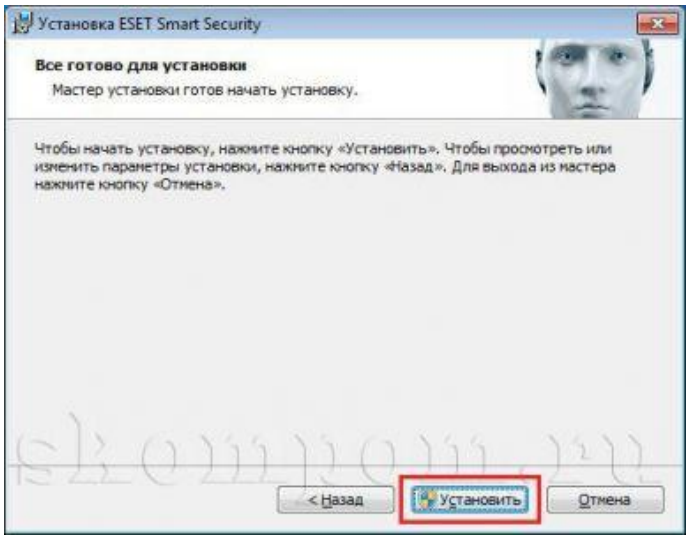
Мен доимо сизларга маслаҳат берадиган потенциал исталган дастурларни аниқлашни ўз ичига олади. Кирувчи дастурлар сизнинг ўрнатишни талаб қиладиган ва улар бутун тизимингизнинг ишлашига сезиларли таъсир қилиши мумкин бўлганлардир. Биз "Кейинги" га борамиз.



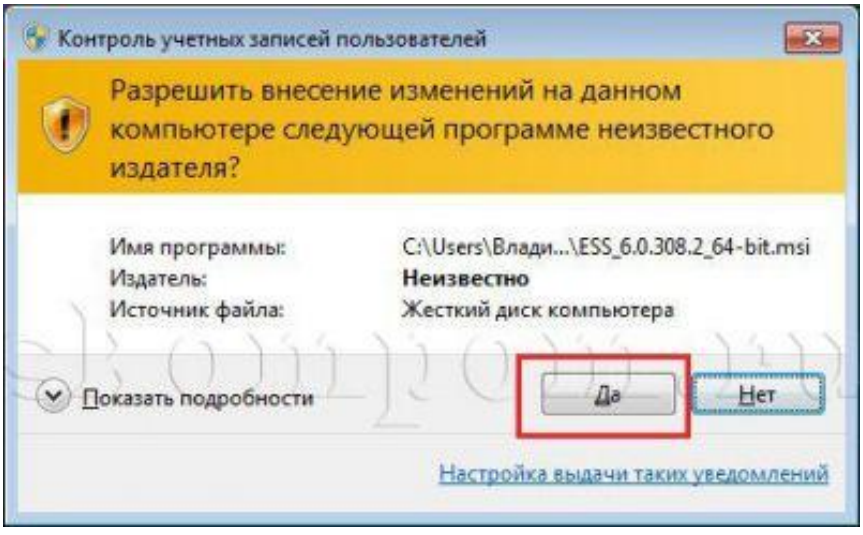
Янги бошланувчилар учун шахсий чиқиш деворининг "Автоматик режими" ни тарк этишни тавсия этаман, унда стандарт чиқиш ҳаволалари ўчирилади ва ишга туширилмайди - ўчирилмайди. "Next" тугмасини босиб ESET Smart Security дастурини ўрнатишни давом этамиз.



Кейинги ойнада "Устонавить" тугмасини босамиз.

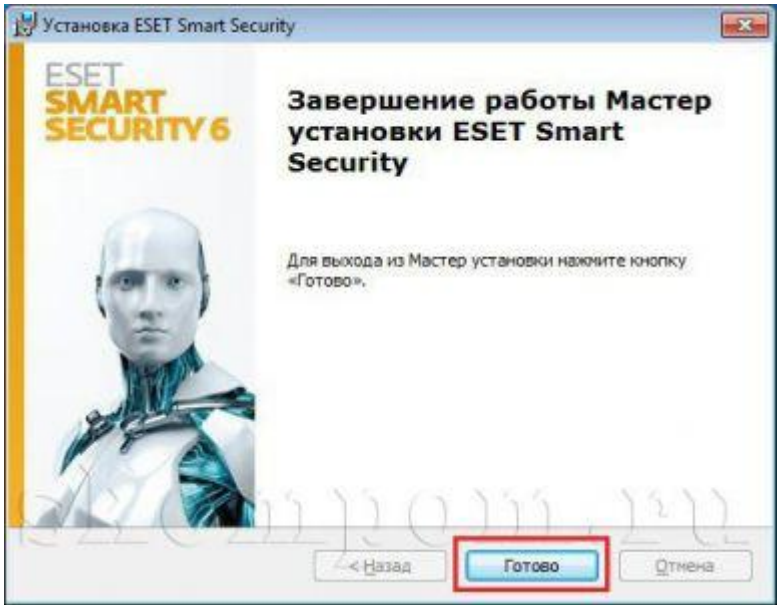


Шундан сўнг, тизим ўрнатилган дастурнинг компютерда ўзгаришларни амалга оширишга рухсат беришни хоҳлайсизми, деб сўрайди. Сичқончанинг чап тугмаси билан "Ҳа" тугмасини босиш орқали розилик берамиз.

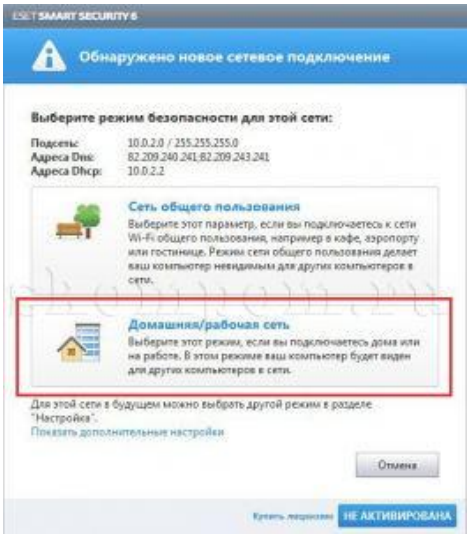


Антивирусни ўрнатиш жараёни бошланади.

Кейинчалик ESET Smart Security Ўрнатиш Сиҳирбазани ёпилиши ҳақида хабар билан бир ойна пайдо бўлади. "Бажарилди" тугмасини босинг.



Шундан сўнг тизимингизда шахсий хавфсизлик девори аниқланади тармоқ уланиши ва ушбу тармоқнинг хавфсизлик режимини танлашимизни талаб қилади. Агар биз жамоат жойида тармоққа уланишни ишлатаётган бўлсак, "Умумий тармоқ"ни танлаймиз, шунда компютеримизни ушбу тармоқнинг бошқа фойдаланувчиси кўриши мумкин эмас. Уй учун, Уй тармоғи". Бундай ҳолда, бизнинг компютеримиз бир хил тармоққа уланган бошқа фойдаланувчиларга кўринади. Биз стол компютеридан фойдаланамиз, шунинг учун ҳар доим "Уй Тармоқ" ни танлаймиз.



Ушбу ойнанинг майдони кўрсатилади ESET ни фаоллаштириш Smart Security. ESS ни бепул ишлатишимиз учун биз ўнг томондаги юқори бурчакда ёки пастдаги «Отмена» ёки «Бекор қилиш» тугмачасини босиш орқали активизация билан ойнани ёпамиз.

Ҳозиргача ўрнатилган ESET Smart Security антивирус дастури ишга туширилади. Nod32 антивирусини ўрнатиш ёки ESET Smart Security муваффақиятли бажарилди.

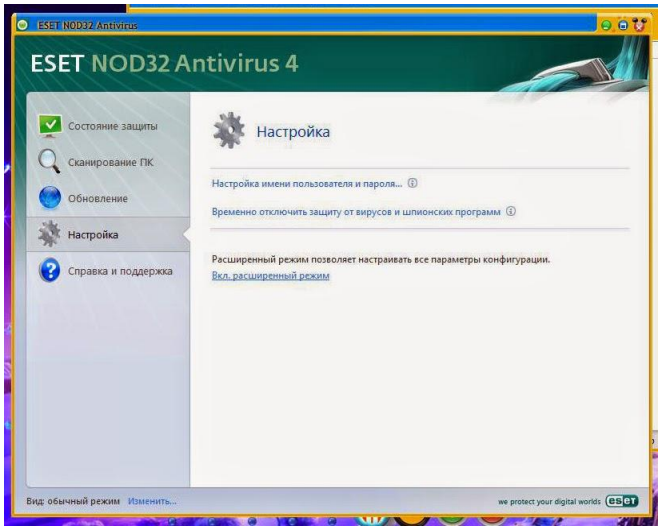
Антивирус базасини янгилашнинг икки хил усули мавжуд:

1. Тайёр база жилдидан янгилаш;
2. Интернетдан база манзилини топиб янгилаш.

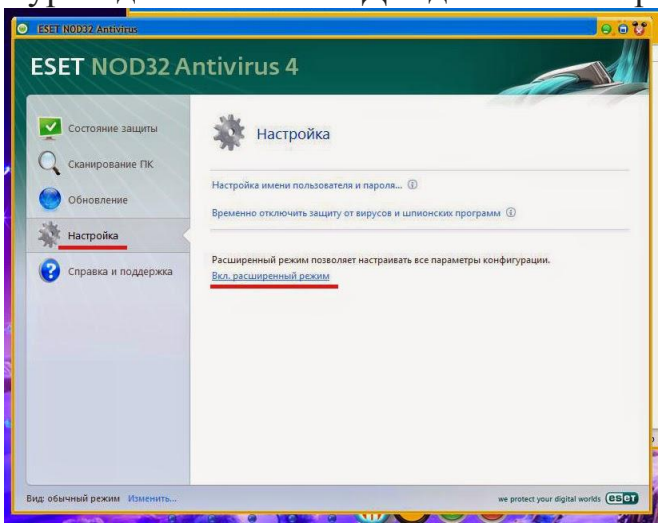
Бунинг учун бизда база жилди бўлиши керак. Аввал база жилдини (бизда у **"nod_upd"** деб номланган, у сизда бошқача номланган бўлиши ҳам мумкин) **“Рабочий стол”** (**"Иш столи"**)га **“Вставит”** (**"Қўйиш"**) қиламиз, сўнгра уни очамиз. Сўнгра **Аддресс**: деган жойдаги жилднинг йўли кўрсатлилган жойни белгилаб уни охирига дроп **(\)** белгисини қўйиб, ҳаммасини белгилаб нусха оламиз (**Копировать**). Агар интернетдан янгиламоқчи бўлсангиз, янги текин базага линкни http://chingachgook.net

топиб, ўша линкдан нусха олишингиз керак бўлади. Бу саҳифада тез-тез нод базаларига линкларни ўзгартириб туришади. Имкон бўлса шу саҳифани браузерингиз хатчўпларига қўшиб қўйинг.

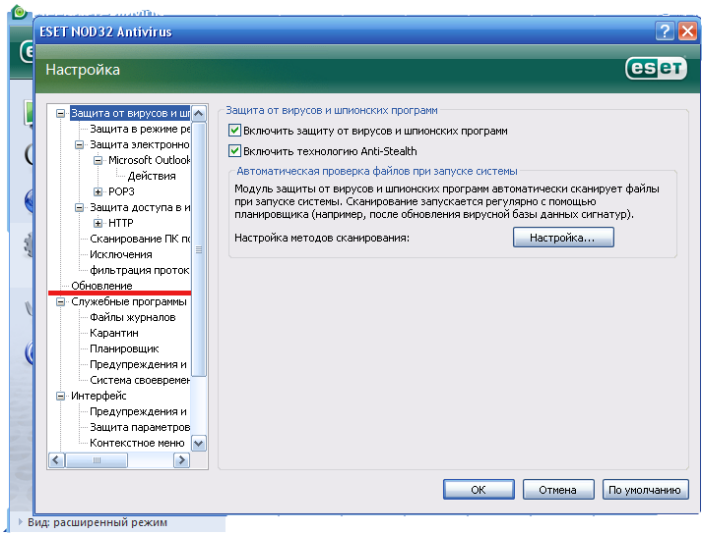
Компутернинг ўнг паст бурчагидаги **“Nod32”** нинг нишонча (белгиси)сини очасиз.



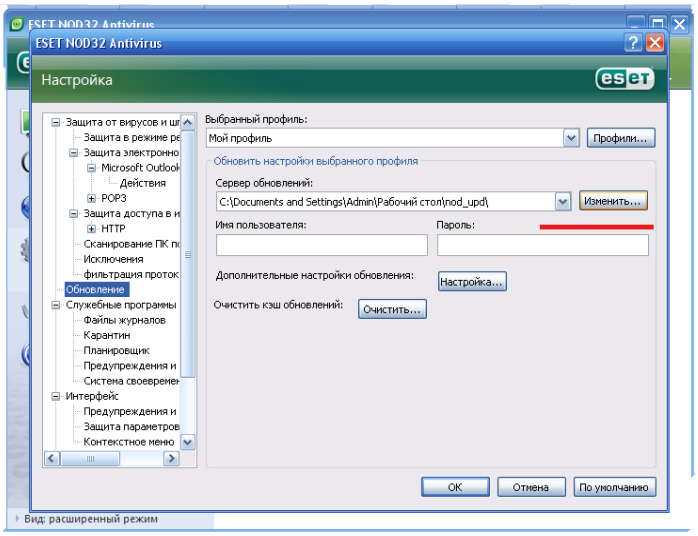
“**Настройка**” вкладкасига кириб, бу ердан "Вкл. расширенный режим" га босамиз ва биздан сўраладиган саволга "Да" деб жавоб берамиз.



Энди у ердан **“Ввод всего рассширенних параметров”**га босамиз.

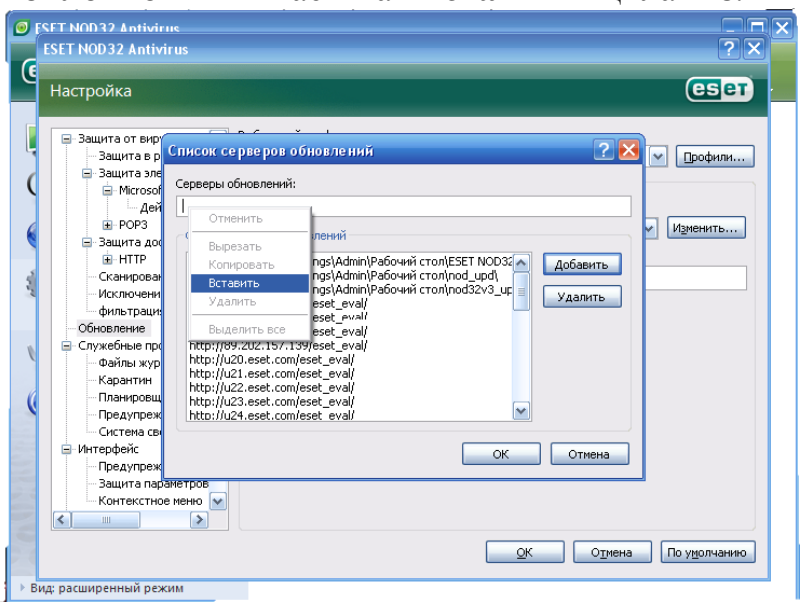


У ердан “**Обновление**” га босамиз.



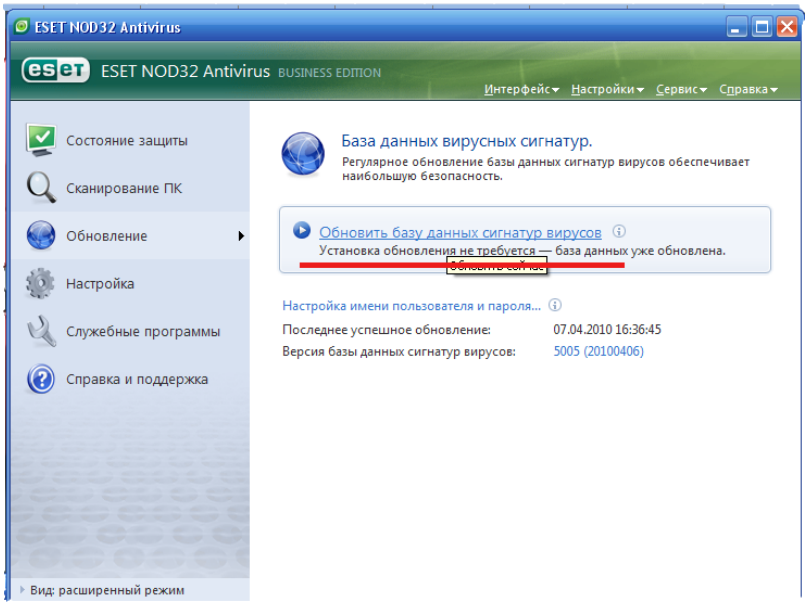
У ердан “**Изменить**”га босамиз.

“Сервер обновление” нинг пастига “**Вставить**” қиламиз.



Сўнгра **“Добавить”**ни, сўнгра **“ОК”**ни босасиз. **“Обновление”** вкладкасига кириб, **“Обновить базу данных сигнатур вирусов”** ни босамиз.

Натижада қуйидаги ойна ҳосил бўлади. Шундан сўнг антивирус базаси янгиланадаи.



ХУЛОСА

Таълим олувчи ўзининг ўқув жараёнида эгаллаган билимларидан, касбий кўникма ва малакаларидан ҳиссий қониқиш ва ундан қувонч ҳиссини ҳосил қилиши лозим.

Ўқувчиларнинг ўқув фаолияти шахсий моҳият сифатида қабул қилинадиган ўқув мақсадларига онгли равишда қаратилган бўлиши лозим. Ўқув фаолиятининг асосий мотивлари ички ўқув-билиш мотивларидир. Ўқув фаолиятининг энг муҳим мотивацияси эса, таълим олувчининг бўлғуси касбига бўлган қизиқиши ва мойиллигидир.

Вазифаларни ҳал қилишда ўқитиш жараёнида компетенциявий ёндошувга асосланган таълимни жорий қилиш улкан аҳамият касб этади. Компетенциявий ёндошувга асосланган таълимни жорий қилиш таълим жараёнида барча иштирокчилар мулоқотнинг демократик услуби ютуқларидан фойдаланишларига хизмат қилади, таълим олувчиларнинг ижодий кучлари ва қобилиятини ўстиради.

Ҳозирда ўқитувчилар ва ўқувчилар учун ҳар бир дарс мавзусига хос хусусиятларга мувофиқ бўлган информатика ва ахборот технологияси соҳасидаги билимларни амалиётда қўллаш компетенциялари, таълим методларини тўғри танлаш, улардан самарали фойдаланиш йўл-йўриқларини пухта эгаллаш энг долзарб масала ҳисобланади. Ушбу йўналишда мазкур «Ахборотларни ҳимоялаш ва антивирус дастурларидан фойдаланиш» номли услубий кўрсатмада берилган тавсиялардан умумтаълим мактаблари информатика ва ахборот технологиялари фани ўқитувчилари ва мустақил фойдаланувчиларга зарур ёрдам кўрсатишига умид қиламиз.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Ўзбекистон Республикаси «Таълим тўғрисидаги» қонуни ва «Кадрлар тайёрлаш миллий дастури» Ўзбекистон. Тошкент. 1997 йил 29 август.
2. Ўзбекистон Республикаси вазирлар маҳкамасининг 2017 йил 6 апрелдаги 187-сонли “Умумий ўрта ва ўрта махсус, касб-ҳунар таълимининг давлат таълим стандартларини тасдиқлаш тўғрисида”ги қарори.
3. Ўзбекистон Республикаси Алоқа, ахборотлаштириш ва телекоммуникация технологиялари давлат қўмитаси сайти - www.aci.uz.
4. Компьютерлаштириш ва ахборот-коммуникация технологияларини ривожлантириш бўйича Мувофиқлаштирувчи кенгаш сайти - www.ictcouncil.gov.uz.
5. Б.Болтаев, М.Маҳкамов, А.Азаматов, С.Раҳмонқулова “Информатика” Умумий ўрта таълим мактабларининг 7-синфи учун дарслик. Тошкент 2017 йил.
6. Б.Ж.Болтаев, А.Р.Азаматов, А.Д.Асқаров, М.Қ.Содиқов Г.А.Азаматова “Информатика” Умумий ўрта таълим мактабларининг 9-синфи учун дарслик. Тошкент 2015 йил.
7. Арипов М, Хайдаров А. “Информатика асослари”. Академик лицей ва касб–ҳунар коллежлари учун ўқув қўлланма – Т.: “Ўқитувчи”, 2002 йил.
8. Арипов М., Р.М.Ирмуҳамедова, М.В.Сагатов, А.Т.Ҳайдаров, А.Х.Якубов, Т.Имамов. “Информатика Ахборот технологиялари” 1-қисм. Тошкент “Университет”, 2007 йил.

МУНДАРИЖА