

**АХБОРОТ
ХАВФСИЗЛИГИНИ
ТАЪМИНЛАШ**

Ахборот хавфсизлиги турлари

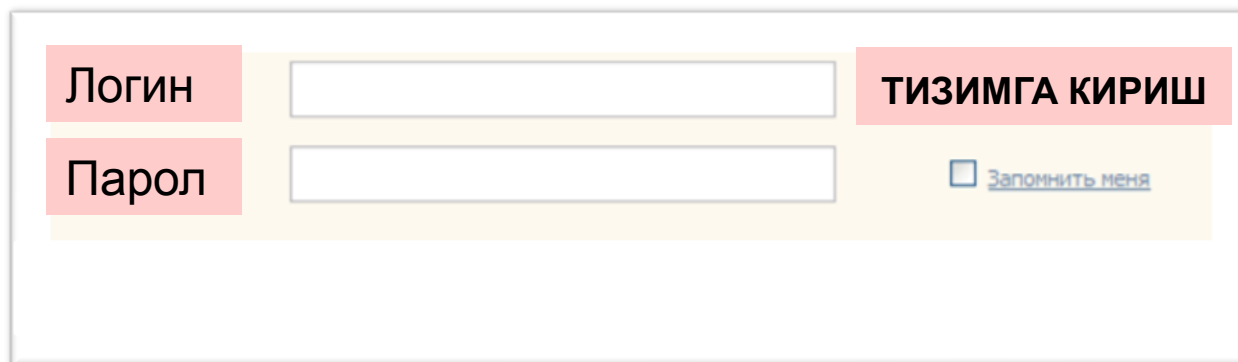
- Ахборот хавфсизлигининг ташкилий чоралар
- Ахборот хавфсизлигининг техник чоралари
- Ахборот хавфсизлигининг дастурий чоралари

Ахборот хавфсизлигини таъминлаш

- *Ахборот хавфсизлигини таъминлаш* – бу фойдаланувчининг ахборотларини ҳимоялашга қуйилган меъёр ва талабларни бажаришидир.
- *Ахборот хавфсизлиги* – бу ахборот фойдаланувчиларига ва кўплаб ахборот тизимларига зарар келтирувчи табиий ёки сунъий характерга эга тасодифий ва уюштирилган таъсирлардан ахборотларни ва ахборот коммуникация тизим объектларининг ҳимояланганлигидир.

Логин ва пароль тушунчаси

- **Логин** – шахсинг, ўзини ахборот коммуникация тизимига таништириш жараёнида қўлланиладиган белгилар кетма-кетлиги бўлиб, ахборот коммуникация тизимидан фойдаланиш ҳуқуқига эга бўлиш учун фойдаланилувчининг махфий бўлмаган қайд ёзуви ҳисобланади.
- **Парол** – унинг эгаси ҳақиқийлигини аниқлаш жараёнида текширув ахбороти сифатида ишлатиладиган белгилар кетма-кетлиги (махфий сўз). У компьютер билан мулоқот бошлашдан олдин, унга клавиатура ёки идентификация картаси ёрдамида киритиладиган ҳарфли, рақамли ёки ҳарфли-рақамли код шаклидаги махфий сўздан иборат.



The diagram shows a login form with two input fields and two buttons. The first row contains a label 'Логин' (Login) on the left, an empty text input field in the center, and a button labeled 'ТИЗИМГА КИРИШ' (Log In) on the right. The second row contains a label 'Парол' (Password) on the left, another empty text input field in the center, and a button labeled 'Заполнить меня' (Remember me) on the right, which includes a small square checkbox icon.

Идентификация ва аутентификация

- **Идентификация** (ингл. *Identification*) – ахборот тизимлари объект ва субъектларига уни таниш учун номлар (идентификатор) бериш ва берилган ном бўйича солиштириб уни аниқлаш жараёни.
- **Аутентификация** (ингл. *Authentication*) – объект ёки субъектни унга берилган идентификаторга мослигини текшириш ва белгилар кетма-кетлигидан иборат махфий кодини текшириш орқали аслигини аниқлаш.
- **Авторизация** – фойдаланувчининг ресурсдан фойдаланиш ҳуқуқлари ва рухсатларини текшириш жараёни. Бунда фойдаланувчига ҳисоблаш тизимида баъзи ишларни бажариш учун муайян ҳуқуқлар берилади. Авторизация шахс ҳаракати доирасини ва у фойдаланадиган ресурсларни белгилайди.

Рўйхатдан ўтиш тартиби

Рўйхатдан ўтиш – фойдаланувчиларни рўйхатга олиш ва уларга дастурлар ва маълумотларни ишлатишга ҳуқуқ бериш жараёни.

Айрим веб-сайтлар фойдаланувчиларга қўшимча хизматларни олиш ва пулик хизматларга обуна бўлиш учун рўйхатдан ўтишни ҳамда логин ва парол олишни таклиф қиладилар.

Фойдаланувчи рўйхатдан ўтгандан сўнг тизимда унга қайд ёзуви (account) яратилади ва унда фойдаланувчига тегишли ахборотлар сақланади.

Имя

Фамилия

День рождения

Город не обязательно

Пол Мужской Женский

Почтовый ящик

Пароль

Повторите пароль

Если Вы забудете пароль
Мы попросим Вас ответить на секретный вопрос. Также пароль можно восстановить через дополнительный email или мобильный телефон.


Мобильный телефон не обязательно

Секретный вопрос

Ответ

Дополнительный e-mail не обязательно

Профиль на Моем Море
В Моем Море@Mail.Ru легко найти одноклассников, сокурсников и коллег.
 Создать личную страницу на Мой Мир@Mail.Ru

 [обновить код](#)

Код на картинке

Логин ва парол масалалари

- **Логин ва паролга эга бўлиш шартлари.** Бирор шахс ўзининг логин ва паролига эга бўлиши учун у биринчидан ахборот коммуникация тизимида руйхатдан ўтган бўлиши керак ва шундан сўнг у ўз логини ва паролини ўзи ҳосил қилиши ёки тизим томонидан берилган логин паролга эга бўлиши мумкин.
- **Логин ва паролни бузиш.** Логин ва паролни бузиш – бу бузғунчининг бирор бир мақсад йўлида ахборот коммуникация тизими объектларидан фойдаланиш учун қонуний тарзда фойдаланувчиларга тегишли логин ва паролларини бузишдир.
- **Логин ва паролни ўғирлаш.** Логин ва паролни ўғирлаш – бу фойдаланувчиларнинг махфий маълумотлари бўлган логин ва паролларга эга бўлиш мақсадида амалга ошириладиган интернет фирибгарлигининг бир туридир.

Ахборотларни ҳимоялаш

- **Шифрлаш** – бу очик ахборотларни ёпиқ кўринишга ўтказиш жараёнидир. Бу жараён муҳим маълумотларни ишончли жойларда сақлаш ёки уларни ҳимояланган алоқа каналлари орқали узатишда қўлланилади.
- Маълумотларни шифрлаш жараёни иккига бўлинади
 - Шифрлаш (зашифровывания) – махсус алгоритм асосида белгилардан таркиб топган махфий калитни ахборотга қўшиш орқали ахборотни ёпиш;
 - Шифрни очиш (расшифровывания) – махсус алгоритм асосида ахборотдан калитни ажратиб олиш орқали маълумотни очиш;

Ресурслардан рухсатсиз фойдаланиш ва унинг оқибатлари

Ахборот-коммуникация тизимининг ихтиёрий таркибий қисмларидан бири бўлган, ҳамда ахборот тизими тақдим этадиган имконият мавжуд бўлган ресурслардан белгиланган қоидаларга мувофиқ бўлмаган ҳолда, фойдаланишни чеклаш қоидаларига риоя қилмасдан фойдаланиш – бу ресурслардан рухсатсиз фойдаланиш тоифасига киради.

Бундай фойдаланиш натижасида қуйидаги оқибатлар юзага келиши мумкин:

- ахборотнинг ўғирланиши;
- ахборотни ўзгартириш;
- ахборотнинг йўқотилиши;
- ёлғон ахборотни киритиш;
- ахборотни қалбакилаштириш ва ҳ.к.

Компьютер вируси

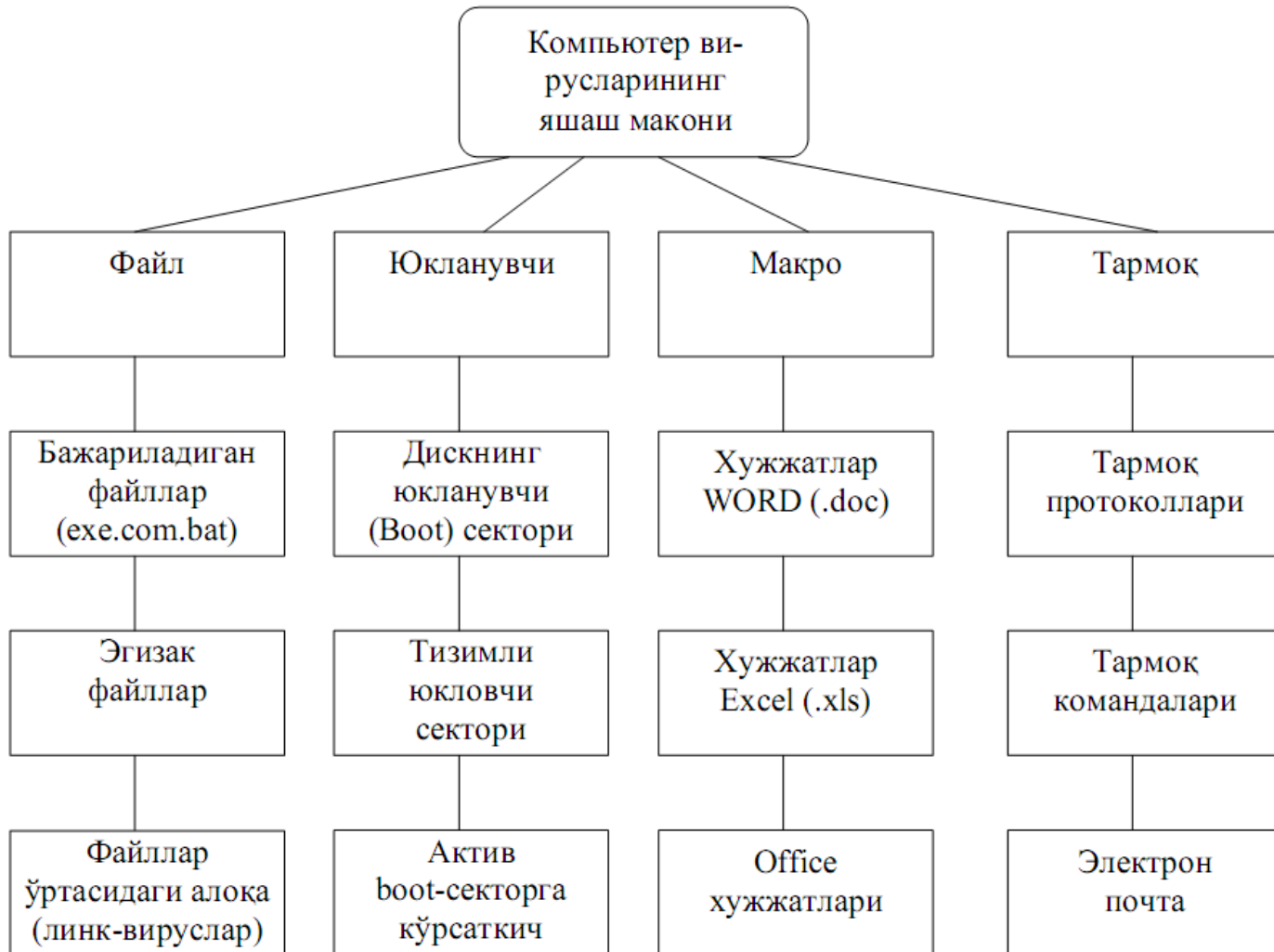
Компьютер вируси – бу ўз-ўзидан кўпаювчи, компьютер тармоқлари ва ахборот ташувчилари орқали эркин тарқалувчи, ҳамда компьютер ва унда сақланаётган ахборот ва дастурларга зарар етказувчи дастур коди ёки командалар кетма-кетлиги ҳисобланади.

Компьютер вируслари қуйидаги хоссаларга эга: ўзидан нусха кўчириш, ахборотдан рухсатсиз фойдаланишни амалга ошириш.

Вирус, аксарият ҳолларда носозлик ва бузилишларга сабаб бўлади ва бирор ҳодиса юз бериши билан, масалан, аниқ куннинг келиши билан ишга туширилиши мумкин.



Вирусларнинг турлари ва вазифалари



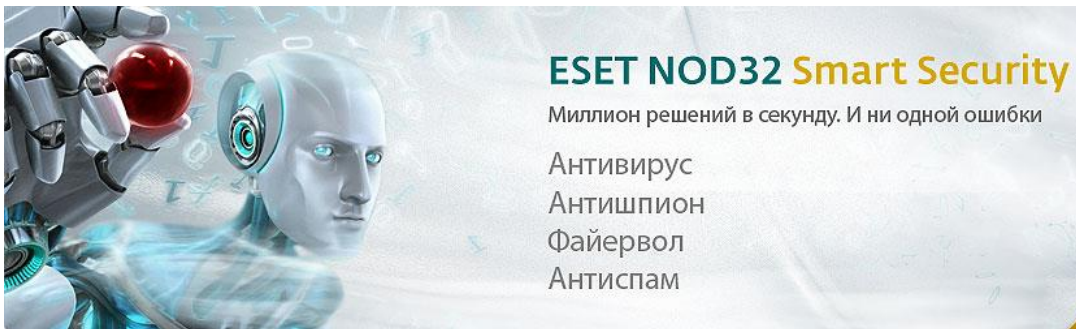
Вирусларга қарши курашиш усуллари

Ҳозирги кунда компьютер вирусларини аниқлаш ва улардан ҳимояланиш учун махсус дастурларнинг бир неча хиллари ишлаб чиқилган бўлиб, бу дастурлар компьютер вирусларини аниқлаш ва йўқотишга имкон беради.

Бундай дастурлар вирусга қарши дастурлар ёки *антивируслар* деб юритилади. Антивирус дастурларига **AVP, Dr.Web, Nod32** дастурларини киритиш мумкин.

Вирусларга қарши курашишнинг асосан қуйидаги усуллари мавжуд:

1. Мунтазам профилактика ишларини, яъни вирусга текширув ишларини олиб бориш.
2. Таниқли вирусни зарарсизлантириш.
3. Таниқли бўлмаган вирусни зарасизлантириш.

The logo for Kaspersky, featuring the word "KASPERSKY" in a stylized green font with red accents, and the Russian letters "КР" in red to the right.

Ҳужум тушунчаси ва ахборот ҳужумлари

Ҳужум тушунчаси – бузғунчининг бирор-бир мақсад йўлида ахборот коммуникация тизимларининг мавжуд ҳимоялаш тизимларини бузишга қаратилган ҳаракати. Бундан фойдаланувчининг логин ва паролини аниқлаш ёки бузиш орқали унинг ҳуқуқларига эга бўлиш.

Ахборот ҳужумлари одатда 3 га бўлинади:

- Объект ҳақида маълумотлар йиғиш (разведкалаш) ҳужуми.
- Объектдан фойдаланишга рухсат олиш ҳужуми.
- Хизмат кўрсатишдан воз кечиш ҳужуми.



UZ-CERT - ТИЗИМИ

UZ-CERT - Служба реагирования на компьютерные инциденты Узбекистана - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

http://uzcert.uz/

Edutest Isoft.uz decanat Olymp Eresms Teach TUIT Software.uz УзАСИ Google @MAIL.RU NEERC-2011 Inmarket WebMoney

UZ-CERT - Служба реагирования на...

UZ - CERT

Сообщить об инциденте

О службе Инциденты Услуги Новости

ВАСКУР.UZ – РЕЗЕРВНОЕ ХРАНЕНИЕ ДАННЫХ

О службе

Авторизация

- Войти

Ресурсы

- [Программа UZ-CERTified](#)
- [SecureSurf](#)
- [Информер UZ-CERT](#)
- [SiteAdvisor](#)
- [Бесплатное программное обеспечение](#)
- [Проверка файлов на вирусы](#)
- [Услуга по резервированию данных](#) **новое**
- [Новости информационной безопасности](#)
- [Законодательство](#)

Служба реагирования на компьютерные инциденты (UZ-CERT) является единым центром для пользователей национальных информационных систем и сегмента сети Интернет, обеспечивающим сбор и анализ информации по компьютерным инцидентам, консультативную и техническую поддержку пользователям в предотвращении угроз компьютерной безопасности.

UZ-CERT является структурным подразделением Центра развития и внедрения компьютерных и информационных технологий UZINFOCOM и в вопросах обеспечения информационной безопасности взаимодействует с ведомственными структурами органов государственной власти и управления Узбекистана.

Служба реагирования на компьютерные инциденты состоит из Группы оперативного реагирования на компьютерные инциденты, Группы анализа, консультаций и программно-технической поддержки и Группы координации и взаимодействия.

Найденные угрозы на веб-сайтах зоны .UZ по месяцам

DATAЦЕНТР UZINFOCOM

Не нужно покупать сервер

Готово

UZ-CERT тизими хизматлари



Участник UZ-CERTified

Адрес сайта: www.tuit.uz

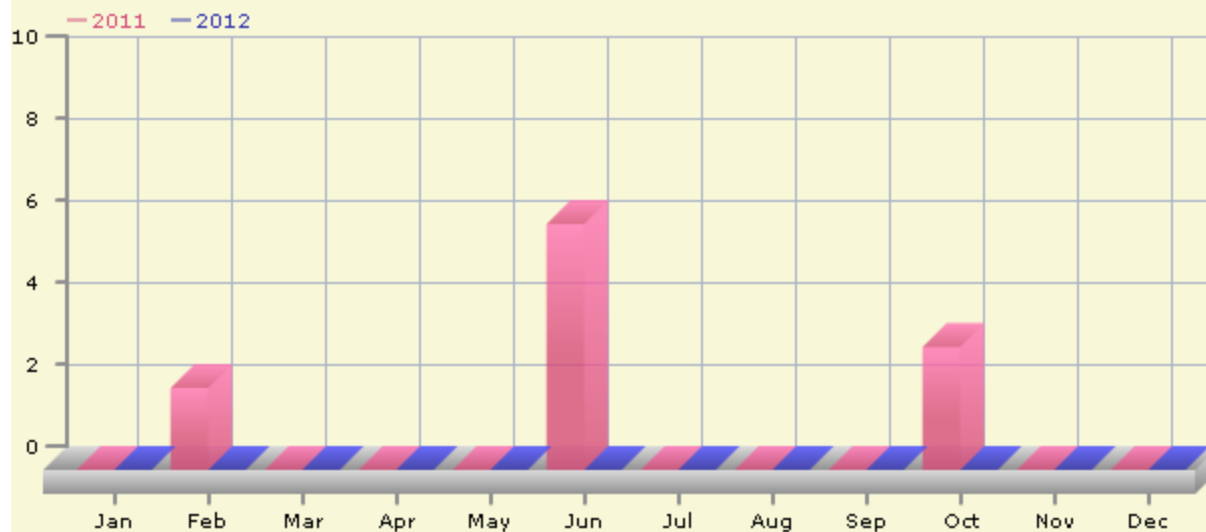
Дата регистрации: 2010-09-21

Последняя проверка: 2011-08-12

[Сведения WHOIS](#)

Новый поиск

Найденные угрозы на веб-сайтах зоны .UZ по месяцам



**Эътиборингиз учун
рахмат!**