|  |
| --- |
| memo grb copy |

ПРЕДМЕТ

< ИНФОРМАТИКА У ЗДРАВСТВУ >

Предавање број 13

**<** **ИНТЕРНЕТ >**

|  |  |  |  |
| --- | --- | --- | --- |
| Недеља | Наставна јединица | Тематске јединице | Резултат – знања или вештине које студент треба да добије |
| 13 | Интернет | Веб маил. Безбедност. Вируси. | Упознавање са веб маил-ом и заштитом од вируса. |

Copyright © 2017 – Факултет медицинских наука Универзитета у Крагујевцу. Сва права задржана. Без претходне писмене дозволе од стране Факултета медицинских наука забрањена је репродукција, трансфер, дистрибуција или меморисање неког дела или читавих садржаја овог документа, копирањем, снимањем, електронским путем, скенирањем или на било који други начин.

Copyright © 2017 – Faculty of Medical Sciences of University of Kragujevac. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying,, recording, scanning or otherwise, without the prior written permission of Faculty of Medical Sciences.

**САДРЖАЈ**

[Е-пошта 2](#_Toc505526714)

[Подешавање програма „Outlook Express“ 2](#_Toc505526715)

[Веб маил 4](#_Toc505526716)

[Разумевање безбедности и безбедног рада са рачунаром 5](#_Toc505526717)

[Проверите свој безбедносни статус у Windows центру активности 5](#_Toc505526718)

[Шта су безбедносна упозорења? 6](#_Toc505526719)

[Коришћење заштитног зида 6](#_Toc505526720)

[Коришћење заштите од шпијунског софтвера 6](#_Toc505526721)

[Аутоматско ажурирање оперативног система Windows 7](#_Toc505526722)

[Вируси 7](#_Toc505526723)

[Шта је вирус и могуће последице 7](#_Toc505526724)

[Начини којима се вирус може пренети на рачунар 8](#_Toc505526725)

[Добре стране апликације за детекцију вируса 8](#_Toc505526726)

[“Дезинфекција” датотека 8](#_Toc505526727)

[Важност редовне надоградње софтвера за детекцију вируса 8](#_Toc505526728)

[Коришћење апликације за детекцију вируса 9](#_Toc505526729)

Предавање бр. 13

**<** **ИНТЕРНЕТ >**

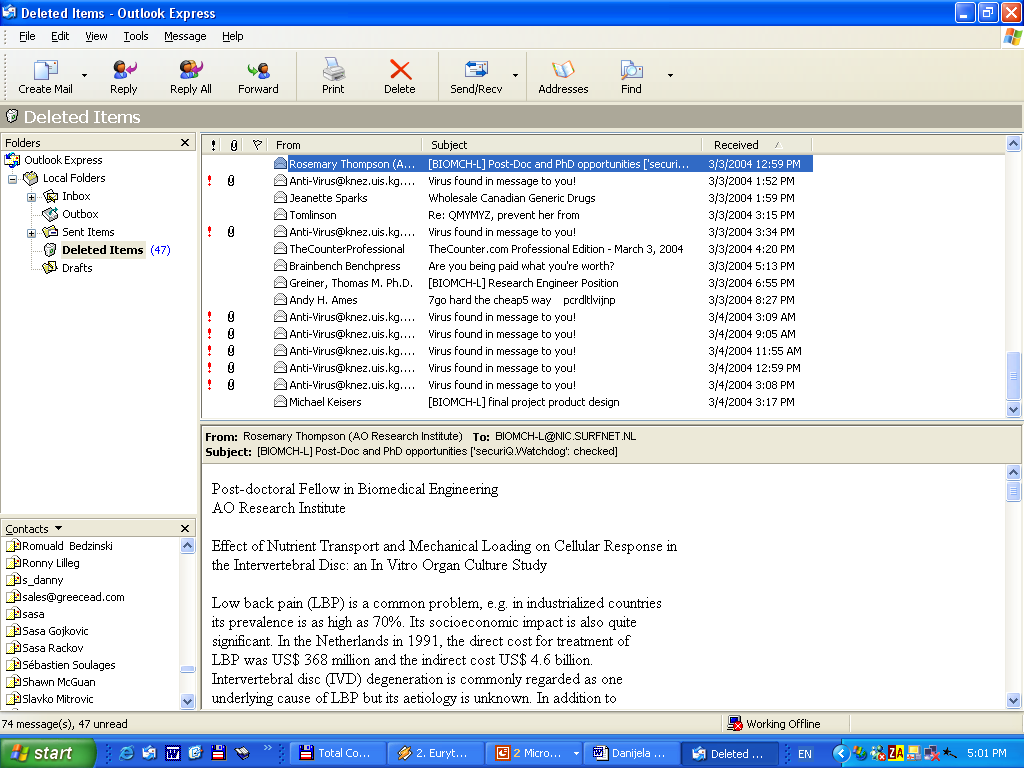
## Е-пошта

### Подешавање програма „Outlook Express“

Један од најпопуларнијих програма за електронску пошту код нас који је долазио са инсталацијом Windows 98/2000/XP је **Microsoft Outlook Express**.

Outlook Express се добија уз Internet Explorer пакет, али се може инсталирати и као самосталан програм. Outlook Express је једноставан и лак за коришћење, па је и то један од разлога што је омиљен међу корисницима.

Inbox Assistant представља могућност да програм сам разврстава пошту на темељу адресе пошиљаоца, кључних речи или нечег другог. Сваки пошиљаоц поруке се може обојити својом бојом тако да је прегледност доста већа, а могуће је и одредити које поруке су за бацање (*Junk* *Mail*), а које поруке корисник не жели ни да види. Иако долази уз Internet Explorer, Outlook Express је потпуно независан од IE. Outlook се подиже сам и не зависи од IE, што за разлику од Netscape-а омогућује већу брзину. Outlook омогућује писање порука у HTML облику, обичним текстом, затим као Word или Outlook докумената, и приказ порука форматираних у HTML-у, које онда могу садржати све што и HTML документи: слике, хиперлинкове, текстове различитих боја и величина.

****

*Изглед прозора Outlook Express при раду са е-маилом - (*[*http://www.microsoft.com/*](http://www.microsoft.com/)*)*

**Рад са порукама**

Свака е-маил порука се углавном састоји од следећих елемената.

***Адресе примаоца поруке***

Пише се у пољу (***То:***) и мора увек бити написана. Уколико поруку шаљемо на више адреса, треба навести све адресе. У овом пољу се може навести адреса или алиас примаоца, која се пише директно или се бира из адресара корисника. Исто важи и за следеће две адресе.

***Адреса примаоца копије поруке***

Овде се наводе адресе особа које нису директно везане за садржај поруке, али треба да знају да је порука послата. Уноси се у поље (***Cc: Carbon Copy***) и није обавезна.

***Адреса примаоца “слепе копије” поруке***

Ови примаоци ће остати невидљиви за оне који су уписани у претходна два поља. Пише се у пољу (***Bcc: - Blind Carbon Copy***).

***Наслов поруке***

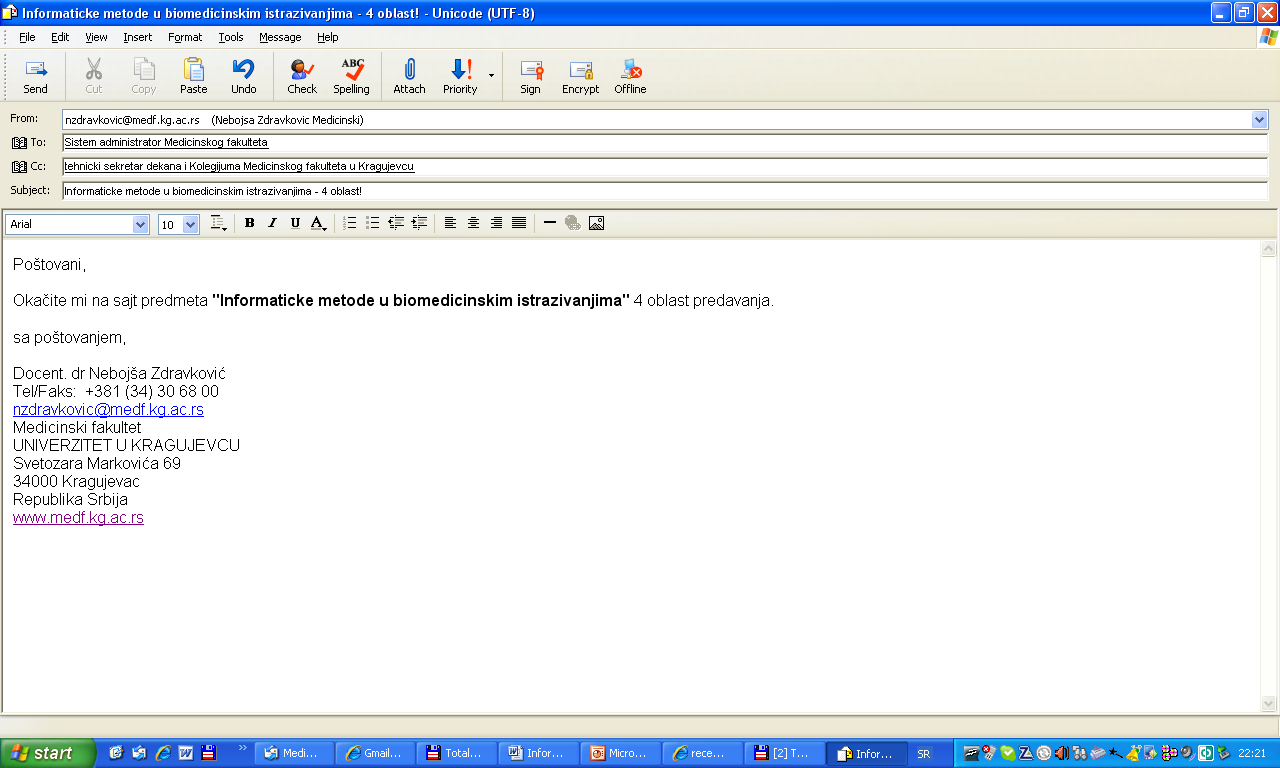
Наслов поруке указује на садржај поруке и треба да буде кратак и јасан (***Subject:***)

***Текст поруке***

У овом прозору се пише садржај поруке.

***Потпис пошиљаоца***

Потпис пошиљаоца (***signature***) није обавезан али спада у општу културу електронске комуникације. Под потписом се подразумева убацивање раније дефинисаног садржаја који представља корисникову подсетницу са именом, титулама, адресом, телефоном, итд.



Изглед поруке у *Outlook Express-у* респективно.

***Прилог поруке***

При слању и примању е-маил порука које садрже прилог треба бити опрезан јер неки од прилога може садржати вирусе. Препоручљиво је овакве поруке најпре проверити да можда не садрже вирусе. Када се пише порука важно је да се адреса тачно напише. Поред тога треба водити рачуна да се не погреши адреса примаоца, па да порука отпутује на погрешну адресу. За успешно слање поруке битно је једино тачно навести адресу примаоца, док сва остала поља (***Cc, Bcc, Subject****),* па чак и текст поруке може остати непопуњен. Избором опције ***Send*** порука ће бити послата. Са опцијом ***Reply*** се директно одговара на примљену поруку, а опција ***Forward*** се користи за прослеђивање поруке другим примаоцима. Тада се аутоматски у поље ***То:*** уписује адреса примаоца, а у поље ***Subject*** ће испред наслова поруке бити додато “***Re:***” односно ***Fw:***

### Веб маил

Веб маил је програм помоћу кога можете читати и слати своју пошту из веб претраживача директно са сервера, где год се у свету налазили. Ово подразумева да можете прочитати своју пошту чак и ако сте конектовани код неког другог провајдера‚.

Да би се добила бесплатна е-маил адреса довољно је доћи на интернет страницу неког од сервиса, попунити тражене основне податке (који не морају бити тачни) и изабрати корисничко име и лозинку. За рад са овом е-маил адресом није потребан софтвер за електронску пошту, већ се све одвија директно на интернет страницама ових сервиса, којима се приступа преко интернет претраживача. Неки од сервиса су потпуно бесплатни или имају дефинисан период бесплатне употребе.

Све у свему, постојање бесплатне е-маил адресе је практично, али корисник мора да трпи разне рекламне поруке. Добра особина бесплатних е-маил сервиса је и то што им се може приступити из било ког краја света, тако да је погодно за кориснике који често мењају место боравка или доста путују. Неки од најчешће коришћених бесплатних е-маил сервиса су:

* <http://www.gmail.com/>
* <http://mail.yahoo.com/>
* <https://www.live.com/>
* <http://www.rocketmail.com/>
* <http://www.mailcity.com/>
* <http://www.forfree.at/>
* <http://webmail.netscape.com/>
* <http://www.operamail.com/>

Сигурно сте чули да је Google један од најпознатијих сајтова на свету. Вероватно сте чули и за ***Gmail***, Google-ов сервис за е-пошту. Све више људи користи ***gmail*** као главни сајт за проверу своје електронске поште. Овде је приказано како да у 4 кратка корака отворите налог на гмаилу и будете као и већина на интернету:

* 1. Отворите страницу <http://www.gmail.com>
  2. Кликните на дугме " ***Sign up for Gmail*** "
  3. Попуните тражене податке (име, презиме, лозинку (минимум 8 карактера), тајно питање итд.)
     1. Уколико сте са српског говорног подручја, а успут вам енглески језик није јача страна, на врху странице имате падајући мени са одабиром језика, па изаберите српски као основни како би вам цела страница са формуларом за регистрацију била на српском језику.
     2. При крају се налази верификација коју морате преписати. Једноставно прекуцајте то што видите исписано накривљеним словима у коцкицу испод слике. Уколико погрешите, мораћете поново попуњавати све податке.
  4. На крају кликните на "***I Accept. Create my account***". Овим прихватате њихова правила о приватности и условима коришћења.

Уколико је све у реду, појавиће вам се страница са честитком да сте успешно креирали ваш налог. На страници је краћи опис ***gmail***-а као сервиса. Да бисте погледали како изгледа ваш нови маил, кликните на дугме "***Show me my account***". Уколико пак није све у реду, проверите шта је означено црвеним словима у формулару и то исправите. Најчешће је лозинка прекратка (мора бити минимум 8 карактера) или је корисничко име које сте одабрали заузето. Када све исправите наставите даље са корацима ка завршетку ове кратке процедуре. Честитам, сада и ви примате електронску пошту на Google-вом сервису ***Gmail***. ***Корисни савети за рад са gmail-ом су окачени на сајту предмета.***

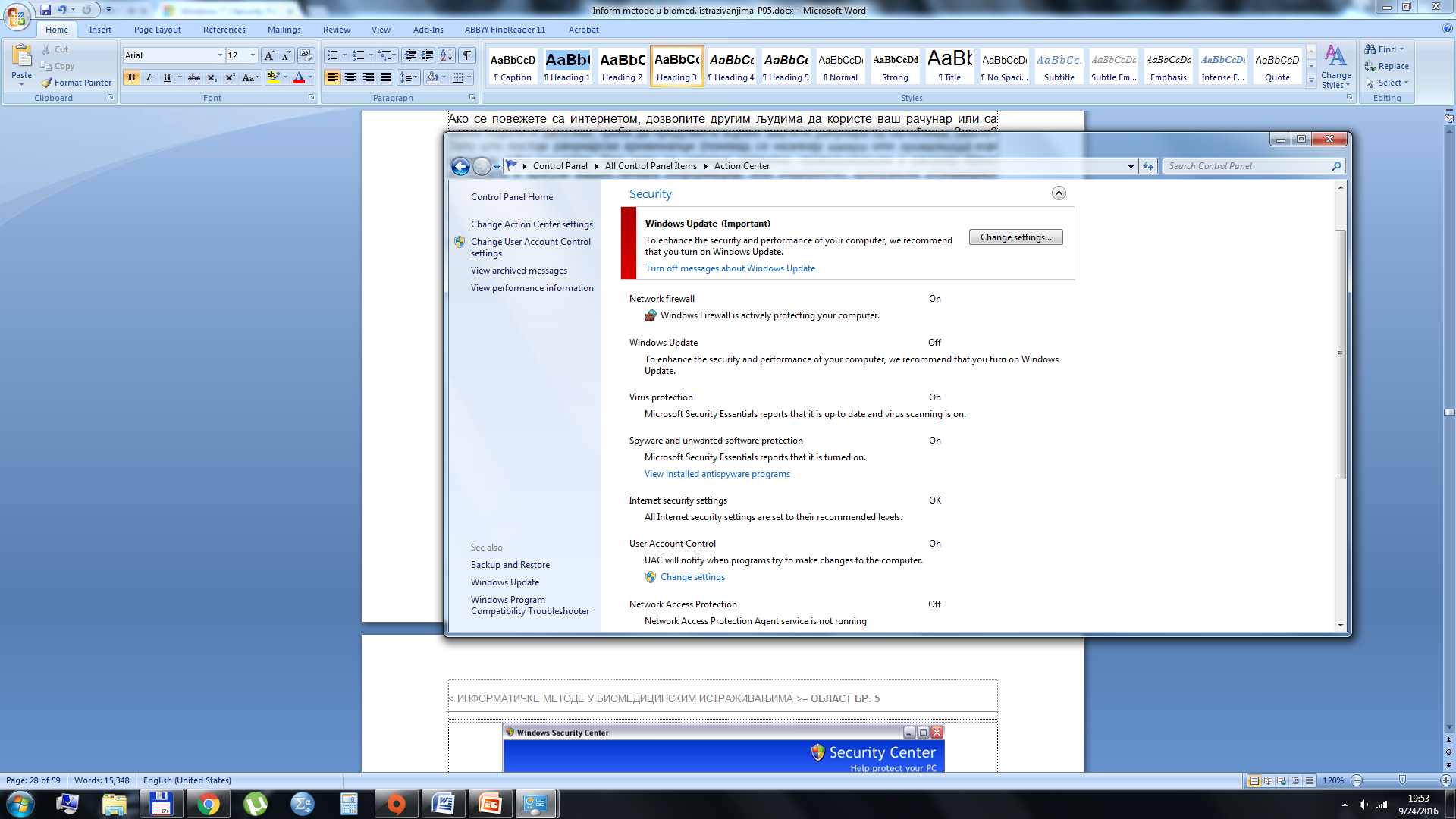
## Разумевање безбедности и безбедног рада са рачунаром

Ако се повежете са интернетом, дозволите другим људима да користе ваш рачунар или са њима поделите датотеке, треба да предузмете кораке заштите рачунара од оштећења. Зашто? Зато што постоје рачунарски криминалци (понекад се називају *хакери* или *провалници*) који нападају туђе рачунаре. Они могу да нападну директно, проваљивањем у рачунар преко интернета и крађом ваших личних информација, или индиректно, креирањем злонамерног софтвера (или *малвера*) који је креиран да нашкоди рачунару.

Срећом, можете да се заштитите тако што ћете предузети неколико једноставних мера опреза. У овом делу су описане претње и начини на које можете да се одбраните од њих.

### Проверите свој безбедносни статус у Windows центру активности

Нови Windows 7 центар активности (***Action Center***) у контролној табли (***Control Panel***) вам помаже да проверите да ли је укључен заштитни зид, да ли је антивирусни софтвер ажуриран и да ли је ваш рачунар подешен да се аутоматски ажурира.



*Windows центар акције*

Да бисте га отворили:

* Отворите безбедносни центар тако што ћете кликнути на дугме **Старт**Slika dugmeta „Start“, изабрати ставку **Контролна табла (Control Panel)**, а затим изабрати ставку **Центар акције (*Action Center*)**.

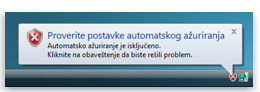
„Центар акције“ проверава ове кључне елементе безбедности на рачунару:

* **Заштитни зид (Network firewall).** Заштитни зид штити ваш рачунар тако што онемогућава приступ неовлашћеним корисницима или злонамерном софтверу.
* **Аутоматско ажурирање (Windows Update).** Windows може редовно да проверава да ли постоје исправке за рачунар и да их аутоматски инсталира.
* **Заштита од вируса (Virus protection).** Антивирусни програм помаже у заштити рачунара од вируса, црва и других безбедносних претњи. Антиспајвер програм помаже при заштити рачунара од шпијунског софтвера и осталог потенцијално нежељеног софтвера.
* **Заштита од шпијунског софтвера (Spyware and unwanted software protection)**. Windows 7 укључује ***Windows Defender***.

Ако je било која од безбедносних ставки искључена, рачунар је можда подложан безбедносним претњама. Да бисте решили проблем, кликните на ставку да је укључите.

### Шта су безбедносна упозорења?

Ако Windows утврди да је рачунару потребно побољшање безбедности у било којој од безбедносних области - код заштитног зида, заштите од малвера или осталим безбедносним поставкама - видећете обавештење приликом сваког пријављивања, које ће бити активно све док се проблем не отклони. Обавештења се приказују на системској траци послова на траци задатака.

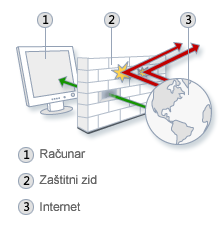


*Обавештење о безбедности*

Кликните на обавештење да бисте отворили „**Центар акције**“ (***Action center*)**, где можете да сазнате како да решите проблем.

### Коришћење заштитног зида

Windows заштитни зид је софтвер или хардвер који проверава информације које долазе са интернета или мреже и затим их одбацује или им дозвољава да прођу до рачунара, у зависности од поставки заштитног зида. На тај начин, заштитни зид помаже у спречавању хакера и злонамерног софтвера да приступе рачунару. Windows заштитни зид је уграђен у Windows и укључује се аутоматски.



*Како функционише заштитни зид*

Ако покренете програм као што је програм за непосредну размену порука или мрежну игру са више учесника која захтева пријем информација са интернета или мреже, заштитни зид вас пита да ли желите да блокирате или деблокирате (омогућите) везу. Ако одаберете да деблокирате везу, Windows заштитни зид креира изузетак тако да вам неће сметати у ситуацији када програм убудуће треба да прими информације.

### Коришћење заштите од шпијунског софтвера

Шпијунски софтвер је софтвер који може да приказује рекламе, прикупља информације о вама или да промени поставке на рачунару, обично без прибављања вашег пристанка. На пример, шпијунски софтвер може да инсталира нежељене траке са алаткама, везе или омиљене локације на веб прегледач, промени подразумевану матичну страну или да често приказује искачуће огласе. Неке врсте шпијунског софтвера не приказују симптоме које можете да откријете, али тајно прикупљају осетљиве информације, као што су веб локације које посећујете или текст који куцате. Већина шпијунског софтвера се инсталира путем бесплатног софтвера који преузимате, али се у неким случајевима рачунар може заразити шпијунским софтвером приликом посете веб локације.

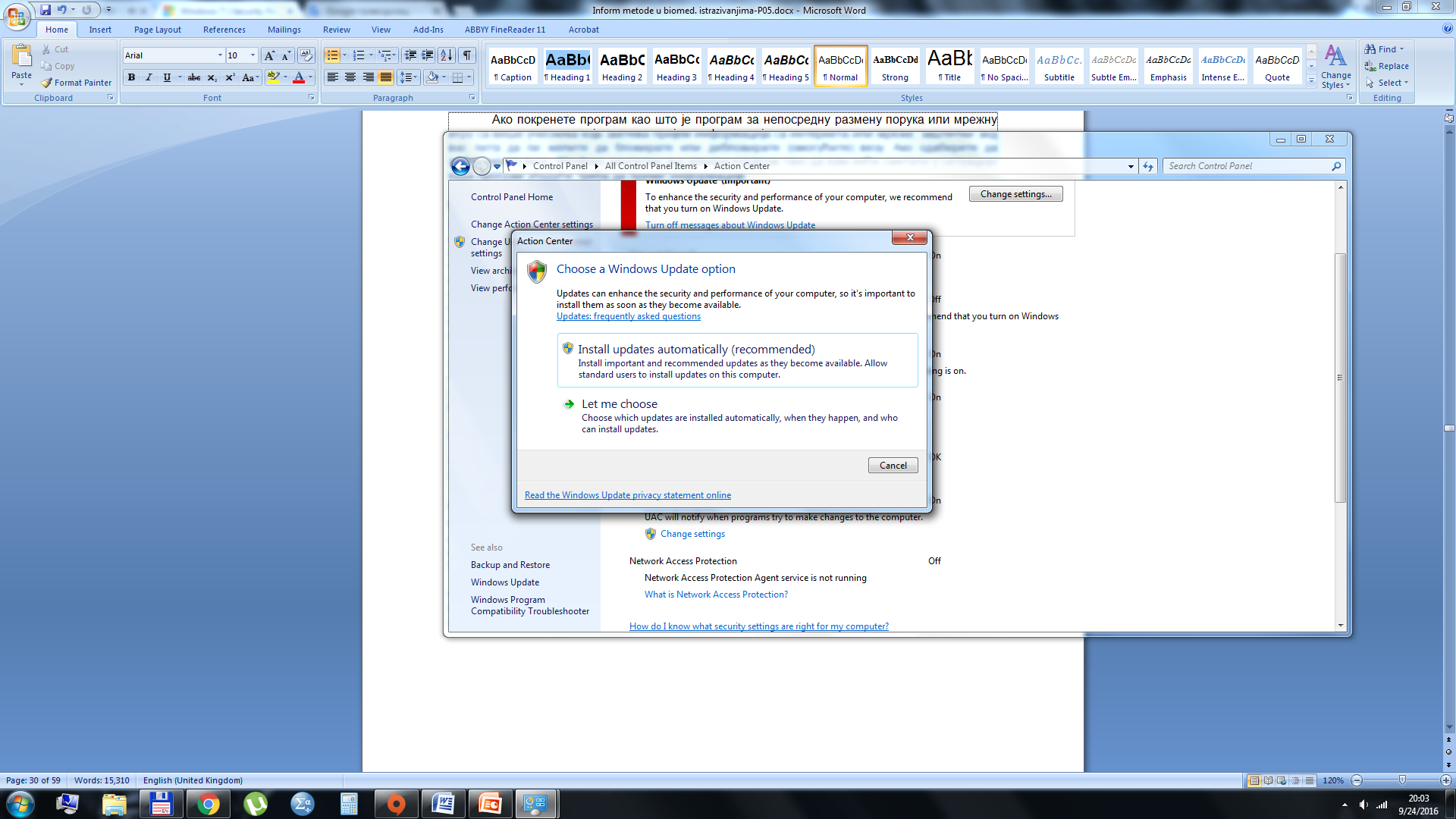
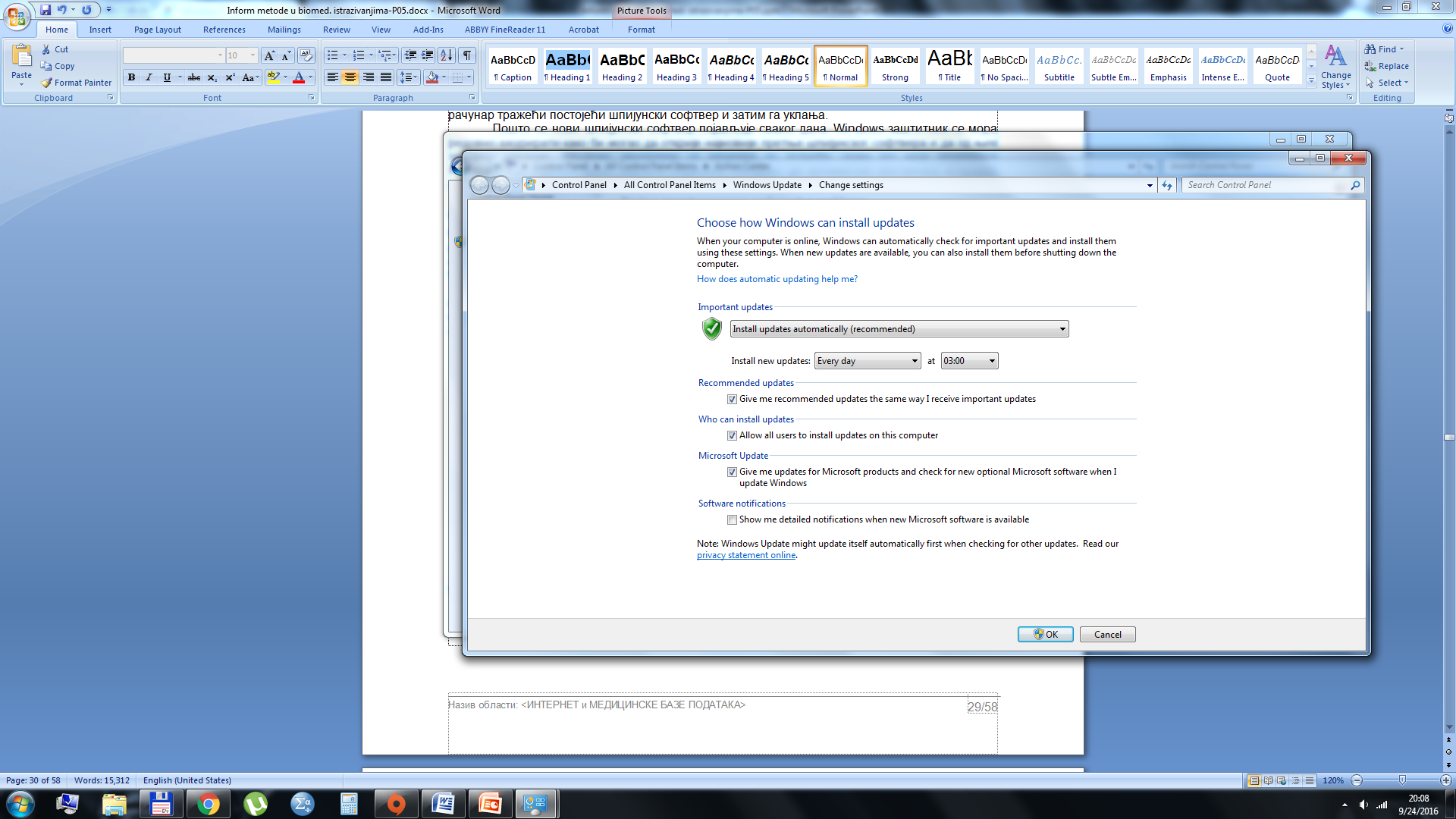
Да бисте помогли у заштити рачунара од шпијунског софтвера, користите антиспајвер програм. Верзија оперативног система Windows Vista има уграђен антиспајвер програм под именом Windows заштитник, који је подразумевано укључен. Windows заштитник вас обавештава када шпијунски софтвер покуша да се инсталира на рачунар. Такође скенира рачунар тражећи постојећи шпијунски софтвер и затим га уклања.

Пошто се нови шпијунски софтвер појављује сваког дана, Windows заштитник се мора редовно ажурирати како би могао да открије најновије претње шпијунског софтвера и да од њих заштити рачунар. Windows заштитник се ажурира по потреби сваки пут када ажурирате Windows. За највиши ниво заштите подесите Windows да аутоматски инсталира исправке (погледајте испод).

### Аутоматско ажурирање оперативног система Windows

Корпорација Microsoft редовно нуди важне исправке за Windows које помажу у заштити рачунара од нових вируса и других безбедносних претњи. Да бисте се уверили да примате ове исправке што је брже могуће, укључите аутоматско ажурирање. На тај начин не морате да бринете да критичне исправке за Windows можда недостају на рачунару.

Исправке се преузимају у позадини када сте повезани са интернетом. Исправке се инсталирају у 3:00, осим ако не наведете друго време. Ако искључите рачунар пре тог времена, исправке можете да инсталирате пре искључивања. У супротном, Windows ће их инсталирати следећи пут када покренете рачунар.

*Аутоматско ажурирање*

**Укључивање аутоматског ажурирања**

1. Отворите функцију „Ажурирање Windows“ тако што ћете кликнути на дугме **Старт**Slika dugmeta „Start“, а затим изабрати ставку **Control Panel**
2. Кликните на икону **Windows Update**
3. Изаберите опцију ***Install updates automatically* (Аутоматски инсталирај исправке-препоручује се)**. Windows ће инсталирати важне исправке за рачунар чим постану доступне. Важне исправке обезбеђују значајне предности као што су побољшана безбедност и поузданост.

## Вируси

### Шта је вирус и могуће последице

Фајлови (програми) који у себи крију злонамерни код зову се вируси. Могу да мењају податке, бришу податке или да неком другом предају контролу над Вашим рачунаром. Постоји више врста злонамерних програма, а најпознатији су вируси, црви и тројанци.

Вируси се каче за програме, чијим покретањем се извршава код вируса. Могу се сами умножавати. Последице су различите - од безначајних сметњи до потпуног уништења података. Вируси се умножавају само приликом покретања заражених програма од стране корисника. Вируси, црви и тројански коњи су хакерски програми који користе интернет да би заразили незаштићене рачунаре.

Црв преузима контролу над функцијама рачунара и аутоматски се шири (копира) без акције корисника. На пример, црв може без знања корисника да пошаље заражене поруке свима чије су адресе у Вашем адресару.

Тројанци, извршавањем на Вашем рачунару, препуштају контролу неком другом, тако да се Вашим подацима може лако приступити преко мреже.

Деструктивни вируси, црви и тројански коњи могу да обришу информације са чврстог диска или да потпуно онеспособе рачунар. Остали не изазивају директна оштећења, али погоршавају перформансе и стабилност рачунара.

### Начини којима се вирус може пренети на рачунар

Највише вируса се шири преко електронске поште у виду прилога. Не отварајте прилоге који стижу од непроверених извора. Велики број вируса се шири и преко програма преузетих са интернета од непроверених извора. Сваки преносиви медиј који добијете, треба прво прегледати на вирусе.

### Добре стране апликације за детекцију вируса

Апликације за детекцију вируса спречавају губитак података. Такође, спречавају смањење брзине рачунара и смањење пропусног опсега интернет везе. Понекад корисници рачунара који немају инсталиран антивирусни софтвер и без свог знања инфицирају велики број других рачунара. Осим тога, ако Ваш рачунар постане заражен, већина електронских порука које шаљете ће бити блокиране и обрисане антивирусним софтвером који штити сервере Вашег интернет провајдера. Антивирусни софтвер спречава да дођете у ситуацију да је Ваш рачунар извор „заразе“.

### “Дезинфекција” датотека

Уклањање злонамерног кода из заражених фајлова зове се дезинфекција. Уколико није могуће дезинфиковати фајлове - треба их обрисати. Ако су заражени фајлови сувише драгоцени да бисте их обрисали, антивирусни софтвер их може сместити у “карантин” тако да не могу да се шире. Неки произвођачи антивирусног софтвера нуде услугу “ручне” дезинфекције заражених фајлова које њихов софтвер није могао да дезинфикује. Можете им послати такав фајл и добити назад очишћену датотеку.

### Важност редовне надоградње софтвера за детекцију вируса

Сваког дана направи се велики број вируса, чак постоје и готови програми за генерисање вируса! Произвођачи антивирусног софтвера, такође свакодневно унапређују своје производе. Важно је да омогућите да се антивирусни софтвер редовно ажурира тј. да са сајта произвођача редовно преузима нове дефиниције вируса. *Windows XP* ће Вас упозорити, ако немате инсталиран антивирусни софтвер или ако тај софтвер није ажуриран.

Неке од адреса произвођача антивирусног софтвера на којима можете пронаћи информације о најновијим вирусима, нове дефиниције вируса, а на некима пребацити на свој рачунар верзије антивирусних програма су:

* *Microsoft Security Essentials (*[*https://support.microsoft.com/en-us/help/14210/security-essentials-download*](https://support.microsoft.com/en-us/help/14210/security-essentials-download)*), бесплатан је за кориснике оперативног система Windows 7*
* *NOD32 (*[*www.eset.com*](http://www.eset.com)*)*
* *Avira,* [*https://www.avira.com/*](https://www.avira.com/)
* *AVG AntiVirus (*[*www.grisoft.com*](http://www.grisoft.com)*)*
* *PC-Cilin (*[*www.antivirus.com*](http://www.antivirus.com)*)*
* *F-Prot (*[*www.complex.is*](http://www.complex.is)*)*
* *Norton Antivirus (*[*www.symantec.com*](http://www.symantec.com)*)*
* *Sophos Anti-Virus (*[*www.sophos.com*](http://www.sophos.com)*)*
* *Kaspersky Anti-Virus (*[*www.kaspersky.com*](http://www.kaspersky.com)*)*
* *McAfee VirusScan (*[*www.mcafee.com*](http://www.mcafee.com)*)*
* *F-Secure Anti-Virus (*[*www.f-secure.com*](http://www.f-secure.com)*)*

Windows нема уграђени антивирусни програм, али је могуће да га је инсталирао произвођач рачунара. Погледајте да ли ваш рачунар има антивирусну заштиту у оквиру апликације „Центар акције“.

Пошто се нови вируси откривају сваког дана, важно је да изаберете антивирусни програм са могућношћу аутоматског ажурирања. Након ажурирања антивирусног софтвера, нови вируси се додају на листу вируса који се надзиру и на тај начин се рачунар штити од нових напада. Ако је листа вируса застарела, рачунар је изложен ризику од нових безбедносних претњи. Исправке обично захтевају годишњу претплату. Обнављајте претплату да бисте редовно примали исправке.

***Упозорење:*** Ако не користите антивирусни програм, излажете рачунар оштећењу од стране злонамерног софтвера. Такође се излажете ризику ширења вируса на остале рачунаре.

### Коришћење апликације за детекцију вируса

Антивирусни софтвер би требало подесити да ради у реалном времену тј. да буде стално активан и прегледава све фајлове које отварате и све програме које користите. Овакво коришћење антивирусног софтвера “троши” ресурсе рачунара и успорава га, али је изузетно корисно.

Антивирусни програми скенирају е-пошту и друге датотеке на рачунару тражећи у њима вирусе, црве и тројанске коње. Ако открије неког од њих, антивирусни програм га *ставља у карантин* (изолује) или га у потпуности брише пре него што оштети рачунар и датотеке.

Све преносиве медије које сте користили на неком другом рачунару, на послу, у школи, итд., треба прегледати на вирусе пре коришћења на Вашем рачунару. Наравно антивирусни софтвер може бити подешен да то ради аутоматски.

Видећемо како се то ради “ручно” тј. према захтеву корисника, помоћу једног од најпопуларнијих антивирусних програма ***NOD32***. Узећемо за пример скенирање дискете. Отвори се Windows Explorer (**Win +е**) и десним кликом на (А:) отвори се контекстни мени. У контекстном менију изабере се ставка NOD32 антивирус сyстем:



Након избора ове ставке NOD32 ће скенирати задату локацију, у овом случају (А:). На следећој слици видимо извештај, да у оперативној меморији и у 58 фајлова, који су на дискети није пронађен вирус.



Може се унапред задати акција коју антивирусни софтвер предузима ако наиђе на вирус. У примеру на следећој слици, задато је да антивирусни софтвер чисти од вируса (***Clean***), а ако то није могуће онда да обрише фајл.

