Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra Informačního Inženýrství

Bakalářská práce

Srovnání antivirových programů pro ochranu dat

Martin Dayef

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Dayef

Informatika

Název práce

Srovnání antivirových programů pro ochranu dat

Název anglicky

Comparison of antivirus software for data protection

Cíle práce

Cílem mé práce je doporučení nejvhodnějšího antivirového programu pro běžného českého uživatele. V teoretické části se zaměřím na specifika vybraných antivirových programů a porovnám je mezi sebou. V praktické části navrhnu řadu testů, které prověří funkčnost programu na ochranu dat. Konečnou analýzou výsledků testů vyhodnotím nejlepší variantu z vybraných programů.

Metodika

Pro testování antivirových programů budou použity nejnovější trial verze lokalizované pro Českou republiku. Pro objektivní posouzení všech vybraných programů proběhne testování na stejné pracovní stanici – náročnost na výkon a chod systému, schopnost rozpoznání škodlivého kódu a otestování množství tzv. falešných poplachů. Operační systém bude před testy pro každý nově použitý bezpečnostní software nahrán znovu do počítače. V závěru srovnám získaná data a seřadím programy z hlediska úspěšnosti v testování. Pro zhodnocení výsledků použiji vícekriteriální analýzu.

Doporučený rozsah práce

30-40 stran

Klíčová slova

Bezpečnost dat, Antivirový program, Vícekriteriální analýza variant

---

Doporučené zdroje informací

BAUDIŠ, P. – ZELENKA, J. *Antivirová ochrana.* Praha: Plus, 1996. ISBN 80-85297-74-4.

HOUŠKA, M. – ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE. KATEDRA OPERAČNÍ A SYSTÉMOVÉ ANALÝZY, – ŠUBRT, T. – BROŽOVÁ, H. *Modely pro vícekriteriální rozhodování.* Praha: Credit, 2003. ISBN 80-213-1019-7.

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 1. 11. 2016

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 11. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 12. 03. 2018

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Srovnání antivirových programů pro ochranu dat" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.03.2018 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Marku Píckovi PhD. za rady a vedení při tvorbě bakalářské práce. Dále bych chtěl poděkovat mým nejbližším za jejich podporu.

Srovnání antivirových programů pro ochranu dat

Abstrakt

Bakalářská práce se zabývá srovnáním antivirových programů dostupných v českém jazyce. Cílem je doporučit vhodnou antivirovou ochranu zařízení běžného uživatele.

Teoretická část je rozdělena do pěti pasáží. První je zaměřena na softwarové hrozby, mezi které patří například malware nebo spam. V druhé jsou popsána rizika hrozící ze stran hardware. Třetí se zabývá prevencí a ochranou před tímto nebezpečím. Další je věnována metodám detekce škodlivého software. V poslední je přiblížena problematika vícekriteriální analýzy variant.

Praktická část je rozdělena na tři kapitoly. Jako první je popsán proces měření. Následuje seznámení s prostředím a funkcemi testovaných programů. Nakonec jsou provedena měření jednotlivých kritérií a okomentovány jejich výsledky.

Na závěr je provedeno zhodnocení celkových výsledků a doporučení nejvhodnější antivirové ochrany.

Klíčová slova: srovnání, test, antivirus, vícekriteriální analýza variant, bezpečnost dat, malware, internet, hrozby, ochrana, detekce

Comparison of antivirus software for data protection

Abstract

This bachelor thesis is focused on comparsion of antivirus software in czech language. The object is to recommend proper data protection for basic user.

The theoretical part of thesis is divided to five parts. The first part is focused on malicious software like malware or spam. The second part describes hardware threats. The third part discuss about prevention and protection. The last part describes malware methods detection and multi-criteria analysis.

The practical part is separated to three sections. The first section describes testing. The second one discusses the user interface and functions of antivirus softwares. The last section is about testing.

At the end is summary of measured values and recommendation which antivirus software should czech user choose.

Keywords: comparsion, test, antivirus, multi-criteria analysis, data security, malware, internet, threats, protection, detection

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

1 Úvod

Žijeme v době, kdy se internet stal nedílnou součástí našeho života. Při čtení emailů, přihlašování se do elektronického bankovnictví, sledování videí, čtení zpráv, sdílení souborů nebo připojování přenosných úložišť na nás mohou číhat potenciální bezpečnostní hrozby. Těmto hrozbám se bohužel někdy nedá předejít, ale můžeme využít celou řadu nabízených antivirových ochran. Z cílené reklamy běžný český uživatel nemůže poznat rozdíl mezi dobrým a špatným antivirovým programem.

Myslím si, že český trh nabízí mnoho kvalitních antivirových programů v různých jazycích a provedeních. Zvolil jsem ty, které jsou dostupné v českém jazyce. Komunikují s uživatelem v jeho rodném jazyce, a tím se stává jejich ovládání snazší, přehlednější a příjemnější.

Díky mému podrobnému srovnání vybraných antivirových programů sestavím objektivní pořadí jejich vhodnosti. Touto prací bych tak rád usnadnil českému uživateli rozhodování při výběru ochrany pro jeho zařízení.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem mé práce je doporučení nejvhodnějšího antivirového programu pro běžného českého uživatele. V teoretické části se zaměřím na specifika antivirových programů, popsání základních hrozeb a využívaných metod pro jejich odhalení. V praktické části navrhnu řadu testů, které prověří funkčnost programu na ochranu dat. Data budu zapisovat a později je využiji na porovnání testovaných antivirových programů. Konečnou analýzou výsledků testů vyhodnotím nejlepší variantu nebo více variant z vybraných programů. Na závěr běžnému uživateli doporučím a popíši vybranou variantu.

2.2 Metodika

Jako první představím bezpečnostní rizika, před kterými nás antivirové programy mají chránit. Následovat budou doporučená preventivní opatření proti těmto hrozbám a popsání metod detekce škodlivého software. Představím také samotné antivirové programy včetně jejich funkcí. Pro testování antivirových programů budou použity nejnovější free a trial verze lokalizované a dostupné pro Českou republiku. Pro objektivní posouzení všech vybraných programů proběhne testování na stejné pracovní stanici – náročnost na výkon a chod systému, schopnost rozpoznání škodlivého kódu a otestování množství tzv. falešných poplachů. Operační systém Microsoft Windows 10 bude před testy pro každý nově použitý bezpečnostní software nahrán znovu do počítače. V závěru srovnám získaná data a seřadím programy z hlediska úspěšnosti v testování. Pro zhodnocení výsledků použiji vícekriteriální analýzu.

3 Teoretická východiska

3.1 Škodlivý software

3.1.1 Malware

Název vznikl spojením anglických slov „malicious“ a „software“, což v překladu znamená škodlivý software. Sám název vypovídá o jeho účelu. Malware je označení pro většinu škodlivých programů, které jsou vytvářené pro krádeže dat a citlivých údajů, převzetí kontroly nad počítačem, šifrování dat za účelem požadování peněžní odměny a dalších činností ohrožujících právoplatného uživatele počítačového zařízení. Jednotlivými typy malware jsou viry, červi, trojské koně, ransomware, adware, spyware, phishing, rootkity a další.

Software se nejčastěji dostává do stanic přes elektronickou poštu a internet. V e-mailových zprávách je součástí důvěryhodně se tvářících zpráv, které obsahují dokumenty, videa a nejčastěji odkazy na škodlivé webové stránky. Internetem se šíří infikovanými soubory, bezplatnými doplňky do prohlížeče, nedůvěryhodnými programy a staženými daty [1], [2].

3.1.1.1 Trojský kůň

Označení vychází z řecké mytologie o Trojské válce. Podle legendy Řekové postavili velkého dřevěného koně, kterého darovali na usmířenou městu Troja. Nevině působícím darem Řekové přelstili trojany, když dovnitř koně schovali vojáky. Vojáci v noci využili moment překvapení, otevřeli brány a mohli se tak zmocnit města. Trojský kůň je na první pohled neškodný program, který je většinou součástí přílohy e-mailové zprávy nebo skrytý uvnitř nějakého instalačního souboru. Do zařízení ho uživatel dostane jako součást něčeho na první pohled neškodného. Na rozdíl od jiného malware se trojský kůň nedokáže bez asistence uživatele sám šířit systémem [2].

3.1.1.2 Vir

Virus je škodlivý software, který se replikuje do jiného programu, spouštěcího (boot) sektoru nebo dokumentu a mění fungování zařízení. Dokáže se šířit, aniž by o tom uživatel věděl. Na rozdíl od červa virus potřebuje, ať už chtěnou nebo nechtěnou, uživatelskou pomoc například ve formě spuštění infikovaného programu. Může být obsažený v příloze e-mailové zprávy, instalačním souboru, na infikované internetové stránce nebo na ní umístěné reklamě. Jakmile virus infikuje hostitelské zařízení, může se šířit dále do systémových programů, nebo aplikační programy upravovat tak, že maže či dešifruje cílová data [8].

3.1.1.2.1 Boot sector viry

Tyto viry napadají spouštěcí část systému na pevném disku (MBR – master boot record). Ta se načítá při spouštění zařízení. Přenáší se převážně externími disky. Po připojení do hostitelského zařízení se vir replikuje do boot sektoru. Jakmile uživatel zapne zařízení, virus se načte do operační paměti. V současné době jsou počítače chráněny opatřeními, která minimalizují riziko napadení sektoru na disku [8].

3.1.1.2.2 Overwrite viry

Jsou v překladu přepisující viry. Zpravidla jsou určeny k ničení souborů a programových dat. Po infikování systému vir začne přepisovat soubory. Může cílit na určité soubory, aplikace nebo systematicky přepíše všechna data na zařízení [8].

3.1.1.2.3 Souborové viry

Některé viry se připojují na programové soubory (většinou typu .exe, .com, .bat). Další mohou infikovat program u kterého je zamýšlena určitá nestandartní operace. (soubory typu .sys, .prg a .mnu). V případě spuštění programu se spustí i vir a může tak vykonat určenou funkci [8].

3.1.1.3 Červ

Počítačový červ je typ škodlivého programu, který má za úkol infikovat další počítače a zároveň zůstat aktivní na napadeném zařízení. Sám se kopíruje na nezasažená místa a jiná zařízení. Nejčastěji využívá části operačního systému, které uživatel

nekontroluje, nebo pro něj nejsou dosažitelné. Dříve se tento druh škodlivého programu šířil zpravidla přes úložná přenositelná média. Po jejich připojení do systému se červ začal replikovat na hostitelském zařízení. Nyní se šíří převážně prostřednictvím sítě, kdy se zachytává na slabiny systému. Může se šířit i pomocí e-mailu, kdy červ automaticky rozešle zprávu všem kontaktům v adresáři. Jsou různé typy tohoto škodlivého programu. Můžou poškozovat hardware, pouze se replikovat nebo znehodnocovat data. Pokud zařízení obsahuje počítačového červa, projeví se to na využití výpočetního výkonu, na běhu operačního systému a na využití programů [7].

3.1.1.4 Spyware

Je to software, který se na výpočetní zařízení dostane bez vědomí uživatele. Většinou se skrývá v instalacích jiných programů. V nejvíce případech je šířen za účelem obohacování. Velmi populární je Keylogger, který zaznamenává jakékoliv stisknutí klávesy a přehled zasílá na určené místo. Bez vědomí uživatele je tak možné zjistit přístupové údaje k účtům na sociální sítě, emailové účty nebo internetové bankovnictví. Může být však využívaný i legálně. V soukromém sektoru, kdy zaměstnavatel instaluje podobný druh spyware na pracovní stanici svého zaměstnance. Je tak schopný sledovat aktivity, které zaměstnanec vykonává (např. navštěvované internetové stránky, doba aktivního využití programů určených k práci apod.). Využití se najde i v domácnosti, kdy rodiče chtějí vědět, jakou činnost na počítači vykonávají jejich děti [2], [6].

3.1.1.5 Ransomware

Je software, který se pokouší v zařízení zašifrovat a zablokovat data. Útočník poté informuje uživatele o možnosti odblokování dat a zařízení zpravidla za poplatek. Většina transakcí probíhá v kryptoměnách (BitCoin, Ripple apod.). Ransomware se většinou šíří přes přílohy v emailových zprávách, aplikace, internetové stránky a externí úložiště. V poslední době se jedná o nejrozšířenější typ malware. Neznámějším ransomware je WannaCry, který v květnu 2017 dokázal infikovat více než 250 000 zařízení na celém světě. Poškodil Národní zdravotnickou službu ve Spojeném království, Deutsche Bahn, Sberbank nebo Telefónica O2 ve Španělsku [10], [11], [12].

3.1.1.6 Adware

Je software, který po spuštění zobrazuje reklamy. Reklamy se zobrazují jako vyskakovací okna nebo tlačítka přímo v grafickém rozhraní programu. Tento typ software lze najít jak na počítačích, tak mobilních zařízeních. Adware nemusí být škodlivý pro zařízení a nepředstavuje nutné riziko. Existují však typy adware, které kumulují osobní údaje nebo sledují zobrazované internetové stránky. Je možné ho získat jako doplněk internetového prohlížeče společně s bezplatným programem nebo přes systémovou bezpečnostní díru. Známé jsou dva druhy programu. Prvním je agresivní adware. Ten zobrazuje reklamu, kdekoliv je to možné. Například při návštěvě internetových stránek se po kliknutí na odkaz zobrazí nespočet oken obsahujících reklamu. Jeho tvůrce chce tímto způsobem získat co nejvíce zobrazení reklamy a s tím spojených peněz. Pro uživatele je tento druh adware velice nepříjemný a obtěžuje ho při využívání svého zařízení. Oproti tomu pasivní adware má pro reklamu vyhrazená místa v aplikaci a není tak pro uživatele natolik obtěžující. Vývojář na druhé straně získá za zobrazení reklamy odměnu [2].

3.1.2 Phishing

Je populární pro svou jednoduchost. Útočník se maskuje za důvěryhodnou instituci (například banky, poštovní společnosti) nebo osobu v emailových zprávách, na sociálních sítích, internetových stránkách a dalších komunikačních prostředcích. Přes ně útočník šíří škodlivé odkazy nebo soubory, které jsou schopné mnoha funkcí. Těmi mohou být získány osobní údaje o uživatelích, přístupové údaje do internetového bankovnictví (čísla bankovních účtů, platebních karet), přístupové údajů na sociální sítě a další služeb. Názorným příkladem je obdržená emailová zpráva odesílaná od bankovní instituce, která příjemce žádá o vyplnění přihlašovacích údajů na odkazované stránce. Nic netušící uživatel po otevření webové stránky vyplní přihlašovací údaje a poskytne tak útočníkovi citlivé údaje, včetně možnosti odcizení peněžních prostředků [17], [18].

3.1.3 Rootkit

Je kolekce programů určená ke vzdálenému ovládání počítače v nevědomí uživatele. Jsou navržené tak, aby útočník získal administrátorská práva pro přístup k zařízení. Na začátku rootkit zajistí uživatelský přístup k počítači. Následuje pokus o prolomení hesel a

zajištění práv administrátora na zařízení nebo dále v síti. Sám o sobě se nedokáže šířit. Bezpečností riziko ovšem představuje. Zpravidla se do počítače dostává instalací bezpečnostních produktů, nevinně působícím rozšířením aplikací nebo spuštěním instalačního souboru z přílohy emailu. Rootkit může obsahovat spoustu dalších škodlivých programů (spyware, backdoor apod.). Není jednoduché odstranit rootkit ze zařízení, a proto je nejlepší obranou preventivní opatření. Je jím například prozkoumání instalovaných součástí programu, odmítnutí navrhované instalace namísto vlastní specifikace nebo aktualizovaný antivirový program a firewall [13], [14].

3.1.4 Spam

Je nevyžádaná elektronická zpráva propagující služby a produkty, která je odesílaná na velké množství emailových adres. Nejde o cílenou reklamu, ale o doručení daného materiálu co největšímu okruhu uživatelů. Odesílatelem je neznámý uživatel. Ve zprávě se často objevuje neexistující adresa nebo email příjemce. Spamem tedy není zaslané reklamní sdělení, se kterým jste souhlasili, například při registraci v internetovém obchodě. Proti nevyžádané elektronické poště se těžko brání a dochází tak v poslední době ke snaze ji omezit legislativou [16].

3.2 Škodlivý hardware

Bezpečnost počítače není ohrožena pouze hrozbami z internetu. Zařízení je možné infikovat i přes hardwarové nosiče dat. Jednou z možností je síťové připojení. Spousta domácností má v dnešní době malou vnitřní síť, na kterou jsou připojené počítače a jiná zařízení. Je tak pravděpodobné, že se škodlivý program na některém ze zařízení bude šířit dále na ostatní zařízení skrze síťové připojení. Další možností jsou přenosná datová úložiště. V dřívějších dobách to byly diskety, poté CD nebo DVD a v dnešní době spíše USB flashdisky nebo externí disky. Škodlivé programy se přes tento hardware přenáší lehce. Stačí, aby uživatel připojil neinfikované přenosné médium do nakaženého počítače a externí zdroj dat je rázem také infikovaný. Externí datový nosič tímto způsobem může nakazit další zařízení, ke kterým bude připojený [20].

3.3 Prevence a obrana

Programy na obranu před škodlivým software jsou účinné, ale stále jsou založeny na algoritmech, které se dají odhadnout a tím i obejít. Použitím více ochranných prvků se samozřejmě zvyšuje bezpečnost zařízení. Je zde ale v hlavní roli člověk jako uživatel. Proto je prevence velmi důležitou součástí při obraně zařízení. Je vždy na uživateli, zda otevře přílohu pochybného emailu od neznámého uživatele nebo zpozorní a přílohy se bezpečně zbaví. Doporučuje se řídit následujícími radami:

- Aktualizovat software. Je nutné aktualizovat antivirové programy, které takto rozšiřují například virovou databázi. Operační systémy obsahují bezpečností díry, které útočníci postupně překonávají a ohrožují tak uživatele. Je potřeba aktualizovat také běžně využívané programy, ty mohou také obsahovat mezery v bezpečnosti a může tak k odcizení citlivých údajů. Většina uvedeného software má možnost automatických aktualizací.
- USB disky a ostatní přenositelná úložná zařízení. Určité typy malware, jako třeba červi, se dokážou kopírovat na jakékoliv USB disky a další přenosná úložná zařízení, které jsou připojené k počítači. Uživatel musí být vždy ostražitý při sdílení úložných zařízení a nejlépe je po navrácení otestovat na přítomnost škodlivého softwaru.
- Hesla. Útočníci se mohou pokusit o prolomení hesla do počítače nebo na jakoukoliv jinou službu. Proto by se uživatel měl při jeho vytváření držet určitých pomůcek. Je důležité, aby silné heslo obsahovalo nejméně osm znaků, včetně velkých malých písmen, čísel a symbolů.
- Nelegálně odemčený (Pirátský) software. Malware je velice často součástí pirátských kopií programů. Při jeho instalaci si můžete nainstalovat škodlivý software.
- Elektronická pošta. Škodlivé programy se často vyskytují v příloze emailu. Uživatel by neměl otevírat přílohu od někoho koho nezná, nebo pokud zpráva působí nedůvěryhodně. Malware se může nacházet i na obsažených odkazech na neznámé internetové adresy.

- Webové stránky. Uživatel by neměl otevírat internetové stránky, které nezná, působí pochybně nebo na ně dostal odkaz od neznámé osoby. Na těchto stránkách se může vyskytovat škodlivý software, který se dostane na počítač při jejich navštívení [3], [4], [5].

3.3.1 Firewall

Název by se dal přeložit jako „bezpečnostní brána“. Může být v podobě hardware zařízení nebo softwaru, který má na starosti oddělovat provoz mezi vnitřní sítí a internetem. Pracuje na základě určených pravidel. Brání před nebezpečnými průniky do vnitřní sítě nebo získávání dat a jejich odesílání na venkovní síť, aniž by o tom uživatel věděl. Nejběžnější formou je software instalace brány na počítač. Společná funkčnost s antivirovým programem je žádoucí a zajišťuje uživateli důležitou bezpečnost. Firewall podle definovaných pravidel povolí služby, které jsou důležité pro běh systému, a ostatní se zakážou. Jako nástroje Firewall se dají uvést SMTP ověřování uživatele nebo IP adresy, kontrola emailů a jejich odesílatelů v seznamech zasílatelů spamu, ověřování existence domény odesílatele. Firewall podrobně sleduje a informuje o dění na internetu. Umožňuje také povolení či zakázání spuštění aplikací. Firewally se mohou rozdělit do tří skupin:

- Paketové filtry – jsou používané na routerech. Mají vysokou rychlost a nízké zabezpečení.
- Aplikační brány – jsou bezpečnější než paketové filtry za cenu menší rychlosti fungování.
- SMLI Gateways – je rychlý s vysokou úrovní zabezpečení [4], [5].

3.3.2 Sociální inženýrství

Sociální inženýrství se provádí za účelem oklamání uživatelů a manipulace s nimi. Cílem je získání cílené informace nebo provedení požadované akce. Útočník se snaží vytvořit u uživatele důvěryhodný dojem. Pro útočníka je výhodou, že nemusí na uživatele útočit nebo dešifrovat hesla. Pomocí vhodných technik získá od uživatele přístupové údaje jednodušším způsobem a může je tak zneužít ve svůj prospěch. Útočník zprvu získá na

první pohled nedůležité informace. Jejich spojením se ovšem dostane na další úroveň informací, které použije k získání těch ještě důležitějších. Oběti tohoto typu útoku často ani nepřijdou na to, že byly zjištěny jakékoliv informace.

Příkladem může být pishingový útok. Uživatel dostane email od odesílatele, který vypadá jako jeho banka. Práva obsahuje na pohled oficiální žádost o otevření uvedeného odkazu a vyplnění přihlašovacích údajů do internetového bankovnictví. Uživatel je v dobré víře vyplní a útočník tak bez větší námahy získá údaje, díky kterým může ukrást peněžní prostředky [18].

3.4 Způsoby detekce škodlivého software

3.4.1 Behaviorální detekce

Zkoumá, jak se chovají a fungují programy. V případě podezřelého chování jako je rozbalování škodlivého kódu, upravování souborů na zařízení a zaznamenávání stisknutí kláves identifikují program jako potenciální nebezpečí. Jak vyplývá, metoda je schopna identifikovat nové hrozby. Ve spojení s heuristickou metodou dokáže klasifikovat podezřelý program jako škodlivý [19].

3.4.2 Detekce signatur

Využívá klíčové aspekty testovaných souborů k vytváření statických otisků již známého škodlivého software. Signatura reprezentuje sérii bytů v souboru. Do databáze se ukládá záznam signatury škodlivého programu. Při testování souborů se porovnávají známé signatury škodlivých programů s testovanými soubory a při shodě je tak objevený infikovaný soubor. Metoda je součástí antivirových programů již od počátku jejich vývoje a je tomu tak dodnes. Problémem této metody je to, že vždy porovnává jen s již detekovaným malware. Útočníkům stačí pozměnit část již známého škodlivého software a metoda má s jeho odhalením problém. Je tak vždy o krok pozadu [19].

3.4.3 Kontrola integrity dat

Kontrola integrity má za úkol hlídat, zda nedochází ke změnám v systémových souborech a dalších důležitých programech. Metoda zaznamenává informace o sledovaných programech a souborech při spuštění systému. Ukládá si je do souboru dat. Ty

pak porovnává se současným stavem souborů. V případě, že se škodlivý program pokusí změnit některý z těchto souborů, kontrola pozná, že došlo ke změně a je tak odhalený. Tím, že kontrola porovnává data o souborech, která si vytvoří sama, je schopná odhalit i nový malware. Úspěšnost této metody také záleží na uživateli jaké soubory a programy nastaví, že chce kontrolovat [21].

3.4.4 Heuristická analýza

Snaží se najít nový škodlivý software pomocí statického testování dat a hledání podezřelých vlastností, které zatím nejsou systému známé. Dokáže také simulovat běh programu, aby zjistil chování tohoto programu po spuštění jestli nevykazuje nějaké podezřelé chování nebo nezpomaluje systém. Jediné podezření však nestačí k tomu, aby byl soubor označený jako nebezpečný. Největší nevýhodou této metody je, že je schopná označit i bezpečný soubor nebo program jako škodlivý [19].

3.4.5 Cloud-based detekce

Na chráněném zařízení provádí sběr dat, která pak analyzuje na vzdáleném systému u poskytovatele služby. Neprovádí lokální testování jako je běžné u většiny metod. Na zařízení je nainstalován antivirový program, který zaznamenává informace o datech a jejich využití. Tato data následně reportuje na vzdálený systém k analýze. Lokálně instalovaný agent minimálně zatěžuje počítač a ponechává mu tak více výpočetního výkonu. Mezi pozitiva patří vytvoření komunity uživatelů a jejich odměňování za identifikaci škodlivého software [19].

3.5 Vícekriteriální analýza variant

Model vícekriteriální analýzy variant řeší rozhodování mezi více variantami a určuje jednu nebo více ideálních variant, které jsou vhodné realizovat. Cílem modelu je vybrat variantu z množiny m variant podle n kritérií. Je možné vybrat nejlepší variantu, která je ohodnocena podle příslušných kritérií, kompromisní variantu nebo pouze určit pořadí všech variant. Pro zajištění nestrannosti při výběru variant je vedle určitých metod a postupů často využíván externí analytik. Jeho využití poskytuje značnou výhodu, protože pro něj neexistuje spojení s výsledkem vybrané varianty. Není proto zatížený touto

skutečností a může postupovat s minimálním zaujetím. Využití externího analytika může být i nevýhodou. Je možné, že nebude dostatečně obeznámený nebo znalý všech detailů a praktické využitelnosti daných variant. Může se tak stát, že bude sice vybrána varianta objektivní, ale prakticky nevyužitelná. Je vhodné znát kvalitu zkoumaných variant. Tu nám pomáhají určit bazální a ideální varianty. Bazální je taková, která je nejhorší možnou variantou příslušného kritéria. Oproti tomu ideální varianta je nejlepší varianta u zkoumaného kritéria. Samy o sobě tyto hodnoty nemůžeme použít při výběru variant, protože bychom dosáhli na nejlepší možný výsledek a mylně bychom ji mohli považovat za optimální variantu [22].

3.5.1 Metoda váženého součtu

Tato metoda na základě kardinálních informací vyhodnocuje funkci užitku pro každou variantu. Díky ní získáme celkové ohodnocení všech variant, které můžeme následně seřadit od nejlepších po nejlepší nebo určit nejvhodnější variantu. Získané hodnoty užitku variant se pohybují v intervalu od 0 do 1 včetně. Čím větší hodnota, tím větší užitek.

Postup výpočtu metody váženého součtu:

1. Je nutné počítat s různorodostí kritérií. Některá mohou být maximalizační (ideální varianta = největší hodnota) a některá naopak minimalizační (ideální varianta = nejmenší hodnota). Pro další výpočet je nutné převést všechna minimalizační kritéria na maximalizační. Pro převod se nejprve vybere maximální hodnota (nejhorší možná) v daném sloupci kritérií. Od té se postupně v každém řádku odečte příslušná hodnota.

2. Zvolíme bazální variantu D a ideální variantu H.

3. Pomocí níže uvedeného vzorce vypočteme prvky ve standardizované kriteriální matici R.

$$rij = \frac{(yij - Dj)}{(Hj - Dj)}$$

4. Následně vypočteme agregovanou funkci užitku pro jednotlivé varianty.

$$u(a_i) = \sum_{j=1}^{n} v_j r_{ij}$$

5. Na konec lze seřadit varianty podle hodnot funkce užitku. Varianta s nejvyšší hodnotou užitku bude nejlepší možnou volbou [22].

3.5.2 Saatyho metoda

V případě, že vybraná kritéria analýzy hodnotí pouze jeden expert, využívá se Saatyho metoda pro stanovení jejich vah. Metoda je založena na principu kvantitativního párového porovnání jednotlivých kritérií. Tato porovnání se hodnotí stupnicí (vždy se hodnotí vztah mezi kritériem *i* a *j*), která je uvedena dále:

- 1 – rovnocenná kritéria
- 3 – slabě preferované kritérium *i* před *j*
- 5 -silně preferované kritérium *i* před *j*
- 7 – velmi silně preferované kritérium *i* před *j*
- 9 - absolutně preferované kritérium *i* před *j*

Preference mezi kritérii se zapisují do Saatyho matice, kde S = (s_{ij}):

$$S = \begin{pmatrix} 1 & s_{12} & \cdots & s_{1n} \\ 1/s_{12} & 1 & \cdots & s_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ 1/s_{1n} & 1/s_{2n} & \cdots & 1 \end{pmatrix}$$

Matice je čtvercová *n*x*n* a platí, že $s_{ij} = 1/s_{ji}$. Tímto se vyjadřují podíly vah mezi *i*-tým a *j*-tým kritériem. Matice má na diagonále vždy jednotkovou hodnotu, protože kritéria jsou si se sebou samými rovnocenná. U matice se provádí i ověření její konzistence I_s, které se vypočte podle vzorce:

$$I_s = \frac{l_{max} - n}{n - 1}$$

l_{max} je zde největší číslo v Saatyho matici a n je počet porovnávaných kritérií. Matice je konzistentní, pokud platí, že $I_s < 0{,}1$. Nejpoužívanější způsob stanovení vah Saatyho metodou využívá geometrického průměru řádků matice a jejich následné normalizace. Pro každý řádek kritéria se stanoví hodnota b_i, podle

$$b_i = \sqrt[n]{\prod_{j=1}^{n} s_{ij}}$$

Na základě hodnoty b_i se stanoví její normalizovaná hodnota v_i, dosazením do vzorce

$$v_i = \frac{b_i}{\sum_{i=1}^{n} b_i}$$

Pro každý řádek kritéria tak vyjde hodnota v_i, kterou považujeme za jeho váhu [22].

4 Vlastní práce

4.1 Proces měření

Měření stanovených kritérií bylo prováděno na přenosném zařízení Lenovo X201. Na jeho pevný disk byl nainstalovaný operační systém Microsoft Windows 10. Pro nasimulování co nejvěrnějšího prostředí běžného uživatele se na disk přesunulo 8 493 souborů v 1 190 složkách. Celkově tyto soubory na disku zabraly 73,9 GB. Mezi kopírovanými daty byly zastoupeny jak větší soubory o velikostech v řádech GB, tak i menší soubory (například fotografie, textové a jiné dokumenty). Data byla převzata z běžně využívaného domácího zařízení. Následně se na pracovní stanici zavedl vždy konkrétní testovaný antivirový program. Další programové vybavení zaváděné nebylo. K zajištění stejných podmínek pro každý z testovaných antivirových programů se vždy před zahájením jejich měření obnovila záloha operačního systému, včetně kopírovaných dat na disku.

4.1.1 Parametry pracovní stanice

Tabulka 1: Parametry pracovní stanice

Komponent	Název	Parametr
Základní deska	Intel Laptop Motherboard 63Y2064	-
Grafický čip	Intel HD Graphics	Integrovaný
Systémový disk (HDD)	Hitachi Travelstar Z7K320	160 GB
RAM (Operační paměť)	Hynix HMT125S6TFR8C-H9	2 x 2 GB, 1333 MHz
CPU (Procesor)	Intel Core i5 M540	2,54 GHz

4.1.2 Testovaná kritéria

Testovaná kritéria byla vybírána s ohledem na preference běžného uživatele. Pro uživatele je jedním z rozhodujících faktorů schopnost rozpoznat škodlivý software. Kvůli bezpečnosti si uživatel antivirovou ochranu zajišťuje, a proto je toto kritérium bráno jako stěžejní. Jako další důležitá kritéria byla vybrána využití výpočetního výkonu, počet chybných oznámení, kvalita a ovládání uživatelského prostředí a rychlost testu zařízení. Přesný výčet je následující:

- využití RAM (operační paměti) – dané kritérium má za úkol zjistit využití operační paměti všemi procesy testovaných antivirových programů. Měření proběhne třikrát při běžném fungování antivirové ochrany. Výpočtem aritmetického průměru z těchto měření bude následně vyhodnocena konečná hodnota kritéria. Pro uživatele je důležité, aby mu při zapnuté ochraně zbyl dostatek volné operační paměti na běžné využití pracovní stanice. Kritérium je minimalizačního charakteru.
- zabraná kapacita na disku – tímto kritériem se sleduje požadavek antivirového programu na volné místo na disku a jeho využití. Měření proběhne zjištěním, kolik program zabírá místa v úložišti při standardní instalaci. Čím méně bude program zabírat místa na pevném disku, tím více bude mít uživatel prostoru pro ukládání osobních souborů. Kritérium je minimalizační.
- vytížení CPU (procesoru) – kritérium sleduje využití procesoru zařízení testovaným programem. Hodnoty kritéria se budou zjišťovat za běžného režimu antivirové ochrany. Každé měření proběhne třikrát a výsledná hodnota kritéria se stanoví výpočtem aritmetického průměru těchto měření. Uživatel má zájem na tom, aby měl k dispozici co největší výpočetní výkon. Díky optimalizovanému programu na ochranu zařízení zbývá více výkonu pro běžnou práci na zařízení. Kritérium je tedy minimalizační.
- rychlost kontroly disku – toto kritérium zjišťuje dobu, za jakou antivirový program stihne provést kompletní kontrolu systému. Proběhnou tři měření času, po které bude probíhat kontrola systému. Výsledná hodnota bude jejich aritmetickým průměrem. Je zřejmé, že má uživatel zájem, aby bezpečnostní kontrola probíhala co nejkratší dobu a kritérium je tak minimalizačního charakteru.
- množství falešných poplachů – zde se sleduje chybovost v detekci škodlivého software. Data měření budou vycházet z provedených testů nezávislým institutem AV-Test. Při přílišném obtěžování uživatele chybnými oznámeními o neexistující hrozbě má uživatel zájem na tom, aby byl počet těchto oznámení co nejmenší. Kritérium je tedy minimalizační.
- schopnost rozpoznání škodlivého software – kritérium zjišťuje úspěšnost v rozpoznání škodlivého software. Jednotlivé hodnoty testovaného kritéria budou vycházet z oficiálních výsledků testů institutu AV-Test. Pro uživatele je důležité, aby antivirová ochrana byla co nejefektivnější v odhalování bezpečnostních hrozeb.

Míra úspěšnosti je uváděna v procentech. Kritérium bude tedy maximalizačního charakteru.

- uživatelské rozhraní – tímto kritériem se ohodnotí ovladatelnost a vzhled uživatelského prostředí. Hodnocení proběhne seznámením se s prostředím antivirového programu a vyhodnocením jeho ovladatelnosti a vzhledu. Bodové ohodnocení kritéria se bude určovat dílčím ohodnocením ovladatelnosti a vzhledu. Za každou část může být program ohodnocený od 0 až do 5 bodů. Celkem tedy půjde získat maximálně 10 bodů. Pro uživatele je důležité, aby byla práce s programem jednoduchá a efektivní. Vzhledem k systému bodování, bude mít kritérium maximalizační charakter.

4.1.3 Určení vah

Stanovení vah jednotlivých kritérií se určilo pomocí Saatyho metody. Metoda spočívá v porovnání preferencí mezi jednotlivými kritérii. Postup řešení této metody je uvedený v teoretické části této práce. Konkrétní přiřazení zkratek ke kritériím je pro přehlednost vypsáno níže:

- K1 – využití RAM
- K2 – zabraná kapacita na disku
- K3 – vytížení cpu
- K4 – rychlost kontroly disku
- K5 – množství falešných poplachů
- K6 – schopnost rozpoznání škodlivého software
- K7 – uživatelské rozhraní

Jednotlivé preference mezi kritérii jsou zaznamenané v následující tabulce. Výsledné váhy jednotlivých kritérií jsou uvedeny v posledním sloupci v_i. Podle předpokladů vyšla nejvyšší váha u kritéria K6, tedy schopnost rozpoznání škodlivého k software. Jak již bylo zmíněno, tak toto kritérium je pro uživatele nejdůležitější, protože kvůli co nejvyšší bezpečnosti si uživatel do zařízení antivirovou ochranu instaluje. Druhou nejvyšší váhu získalo kritérium K1 – využití operační RAM (operační paměti), následované kritériem K3 – vytížení CPU (procesoru) na třetím místě. Předpokládá se, že chce uživatel zachovat co

největší prostor pro běžné využití zařízení. Ten mu zajistí antivirový program s co nejmenším využitím výpočetního výkonu. Kritérium K4 – rychlost kontroly disku má již o značně menší váhu. Běžný uživatel kontrolu provádí většinou v menších intervalech a není proto tak preferovaná jako předchozí kritéria. Stále je ovšem pro uživatele důležitější než K7 – uživatelské rozhraní. V posledních letech se ovšem toto kritérium stává důležitějším než dříve a výrobci chápou, že líbivý vzhled s jednoduchým intuitivním ovládáním je jedním z klíčů ke spokojenosti uživatelů. Následuje K2 – zabraná kapacita na disku, která s navyšováním kapacit úložišť v pracovních stanicích do řádů TB ztrácí na důležitosti. Nejnižší váhu dostalo K5 – množství falešných poplachů. Chybovost v určení škodlivého software je určitě na místě při hodnocení. Příliš časté obtěžování uživatele poplašnými zprávami není žádoucí.

Tabulka 2: Výpočet vah kritérií Saatyho metodou

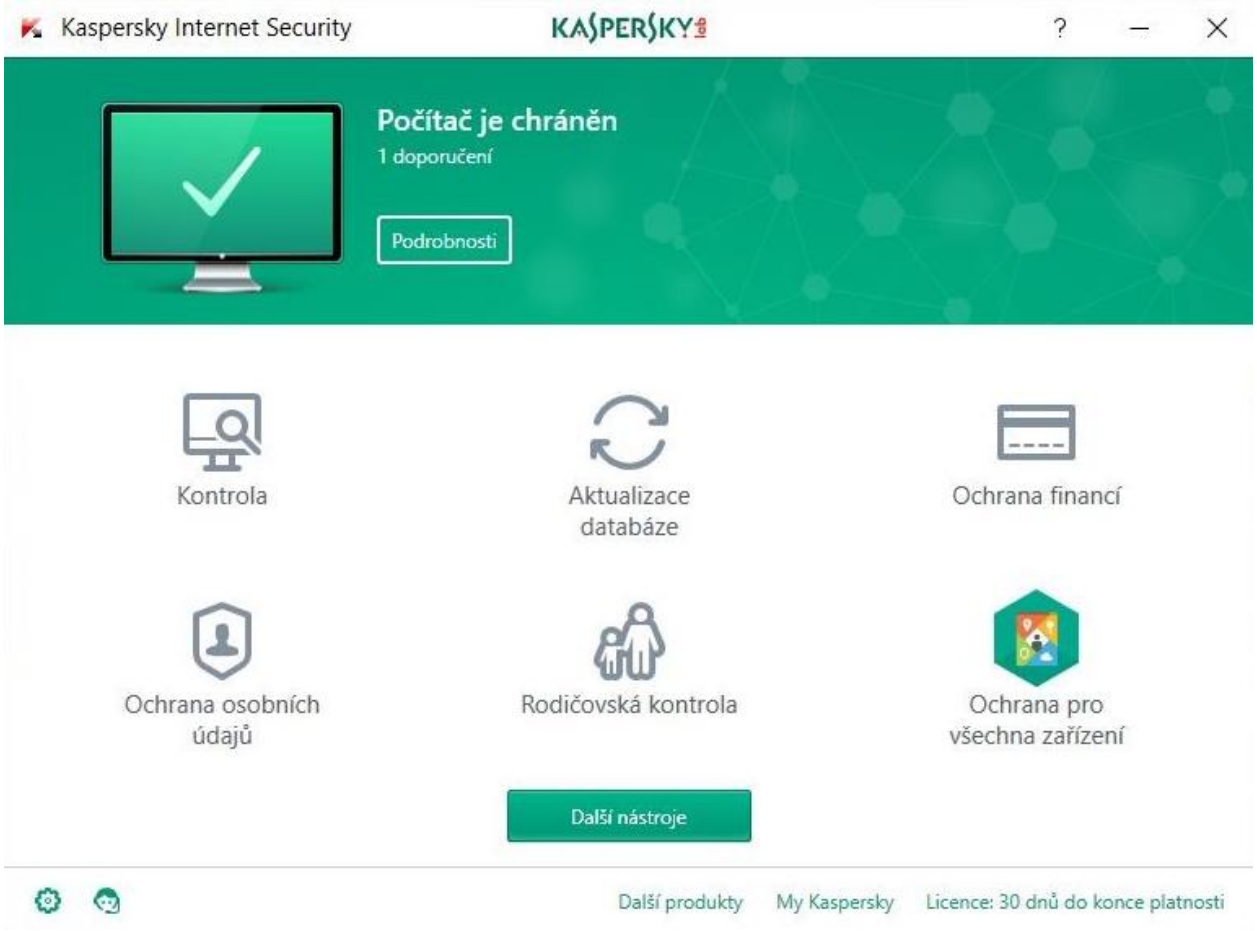
	K1	K2	K3	K4	K5	K6	K7	bi	vi
K1	1	5	3	5	5	1/3	7	2,63	**0,26**
K2	1/5	1	1/5	3	5	1/7	1/5	0,56	**0,05**
K3	1/3	5	1	3	3	1/5	5	1,47	**0,14**
K4	1/5	1/3	1/3	1	3	1/3	3	0,68	**0,07**
K5	1/5	1/5	1/3	1/3	1	1/7	1/3	0,30	**0,03**
K6	3	7	5	3	7	1	7	3,97	**0,39**
K7	1/7	5	1/5	1/3	3	1/7	1	0,57	**0,06**
Suma								10,18	1

4.2 Testované antivirové programy

4.2.1 Kaspersky Internet Security

Výrobcem Kaspersky Internet Security je společnost Kaspersky Lab. Firmu založil Jevgenij Kasperskij v Rusku roku 1997 a je považována za jednoho z největších odborníků v oblasti kybernetické bezpečnosti. Vybraná verze Internet Security je licencována jako trial, tedy zdarma na zkušební dobu 30 dnů. Instalovaný program je ve verzi 18.0.0.405 a v českém jazyce.

Instalace programu trvala několik málo minut a bylo v jejím průvodci možné vybrat, jaké součásti chce uživatel na zařízení nainstalovat. Po prvním spuštění je možné ochranu ihned využívat. Hlavní obrazovka uživatelského rozhraní je rozdělena do tří částí. Ta první je situována v horní sekci rozhraní a obsahuje informaci o stavu ochrany, doporučení antiviru na vylepšení bezpečnosti a správu licence. Nejvýraznější je ovšem prostřední část uživatelského rozhraní. Ta obsahuje celkem šest možností, jak program využít. První z nich je Kontrola, která nabízí kontrolu celého zařízení, rychlou kontrolu, kontrolu nastavenou uživatelem a kontrolu externích zařízení. Další funkcí je Aktualizace databáze, která informuje o aktuálnosti virové databáze a popř. její aktualizace. Ochrana financí je další z nabízených funkcí, která uživateli umožňuje bezpečněji pracovat s internetovými platbami a internetovým bankovnictvím. Další funkcí, na kterou se lze dostat z hlavní obrazovky je Ochrana osobních údajů. Je v ní možné omezit přístup aplikací k webové kameře a zabránit shromažďování informací o aktivitách na webových stránkách. Poslední v hlavní nabídce jsou Rodičovská kontrola, která umožňuje konfiguraci četných omezení uživatelům zařízení, a Ochrana pro všechna zařízení. Díky ní je možné vzdáleně spravovat zabezpečení všech přiřazených zařízení. Mezi prostřední a dolní sekcí uživatelského rozraní je ještě možnost využití dalších doplňků, které Kaspersky Internet Security obsahuje. Jsou jimi například Cloudová ochrana, Aktualizátor softwaru, Bezpečné připojení a další. V dolní části domovské obrazovky je možné přejít do nastavení programu, kontaktovat podporu, zjistit informace o dalších nabízených produktech od výrobce a v poslední řadě také platnost licence. Antivirový software je laděný do zeleno bílého designu a působí jednoduchým dojmem. Ovladatelnost je na dobré úrovni a uživatel se v rozhraní pohybuje vcelku snadno.



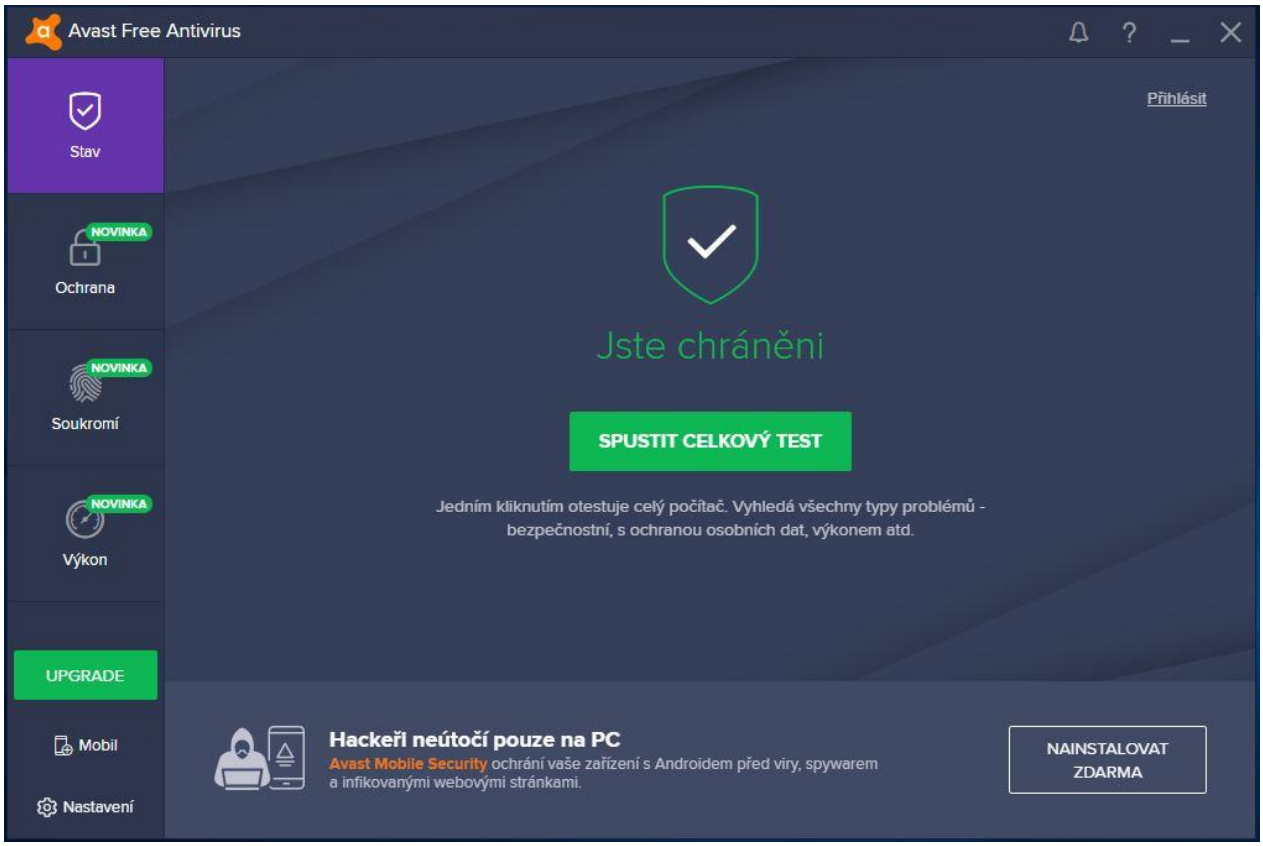
Obrázek 1: Kaspersky Internet Security – uživatelské rozhraní

4.2.2 Avast Free Antivirus

Bezplatný program Avast Free Antivirus začal nabízet jeho český výrobce Avast Software s.r.o. v roce 2002. Jedná se o jeden z nejstahovanějších a nejznámějších bezplatných antivirových programů po celém světě. Program je dostupný zdarma v českém jazyce a byl testovaný ve verzi 18.2.3827.

Instalace probíhá rychle a jednoduše. V jejím průběhu je možné zvolit, jaké doplňky uživatel chce nebo nechce na svém zařízení mít. Program je po dokončení instalace ihned připravený k používání. Na úvodní obrazovce je v jejím středu umístěna aktuální informace o stavu ochrany a možnost okamžitého spuštění celkového testu. Ten otestuje přítomnost škodlivého software, problémy s výkonem zařízení nebo kvalitu hesel. Oznámení a nápověda jsou umístěny nahoře. V dolní části obrazovky se zobrazují nabídky na nainstalování nebo zakoupení dalších programů od výrobce antivirové ochrany. Nejdůležitější ovládací prvky jsou umístěny v hlavním menu na levé straně uživatelského

rozhraní. Jako první je zde položka Stav, která slouží zároveň i jako domovská obrazovka. Druhá v pořadí je Ochrana. Po jejím otevření se uživateli nabídne devět dlaždic s výběrem testů, bezpečnostních štítů, virovou truhlou, inspektorem wi-fi, aktualizací programů a dalšími nabídkami na placený upgrade antivirové ochrany. Další sekcí v hlavním menu je Soukromí. Jediné, co zde uživatel může zdarma využít je správce přihlašovacích údajů, platebních karet a poznámek. Posledním ovládacím prvkem v menu je Výkon, který zdarma nabízí pouze funkci Herní režim. Pokud je režim zapnutý, tak potlačuje oznámení od Avastu, pozastaví aktualizace Windows a snaží se tak zaručit vyšší výkon pro hraní počítačových her. V dolní části hlavního menu má uživatel možnost provést upgrade programu, nainstalovat si antivirovou ochranu na mobilní zařízení a provést nastavení antiviru. Uživatelské rozhraní je dobře uspořádané, má propracovaný vzhled a uživatel se tak nemusí dlouho seznamovat s ovládáním antivirové ochrany.

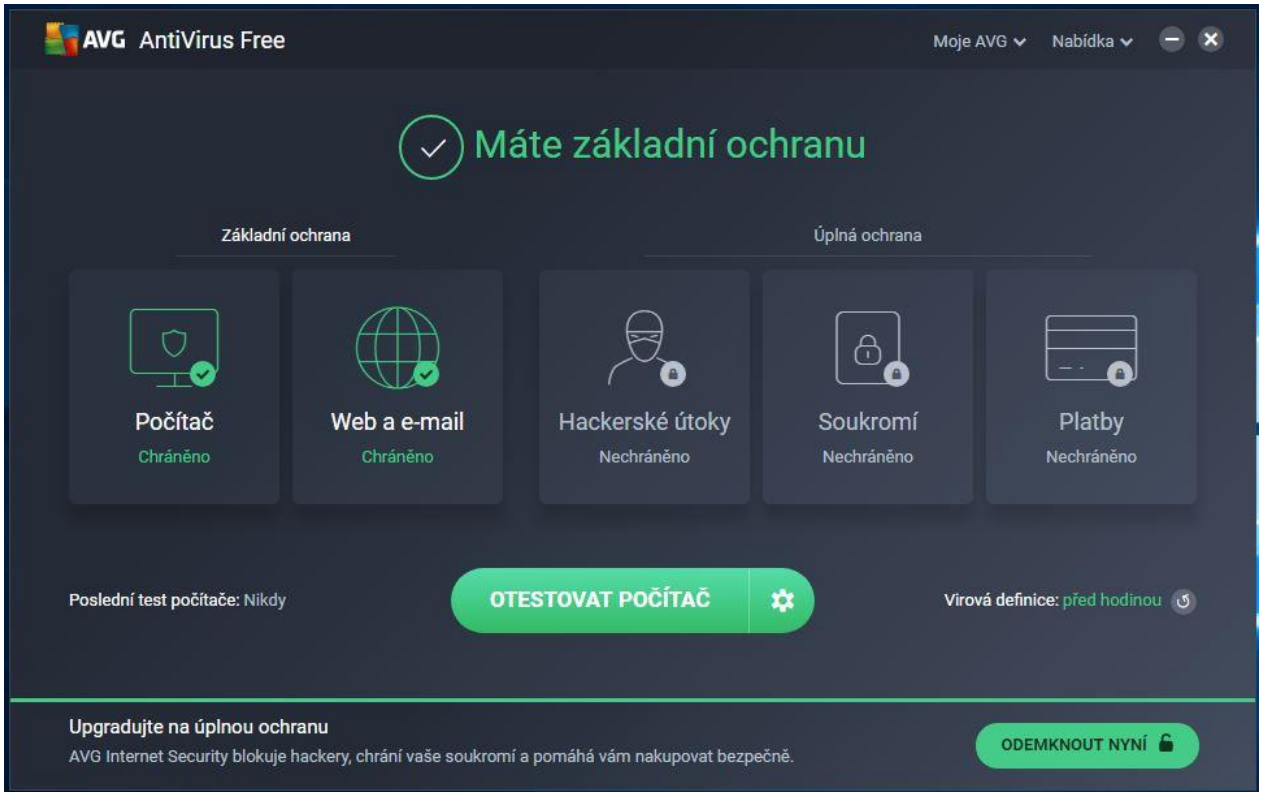


Obrázek 2: Avast Free Antivirus – uživatelské rozhraní

4.2.3 AVG AntiVirus Free

Antivirovou ochranu AVG (název AVG je zkratka spojení Anti-Virus Guard), vyvíjí česká společnost AVG Technologies. Ta byla založena Janem Gritzbachem a Tomášem Hoferem v roce 1991. Bezplatná antivirová ochrana od AVG má tradici již od roku 2000 a dnes patří mezi jednu z nejvyužívanějších. V roce 2016 se za 1,3 miliardy dolarů stala majitelem jiná česká společnost AVAST.

Pro instalaci programu na zařízení stačí stáhnout instalační balíček z oficiální stránky výrobce a provést instalaci. Ta je jednoduchá a rychlá. Program je dostupný v českém jazyce a byl testovaný ve verzi 18.2.3046. Po prvním spuštění antiviru se zobrazí žádost o aktivaci programu. Po jejím rozkliknutí se zobrazí oznámení, že je antivir aktivován a je možné dále pokračovat v jeho využívání. V horní části obrazovky se zobrazuje hláška o stavu zabezpečení. Uprostřed je hlavní nabídka, která je rozdělena na část Základní ochrana a Úplná ochrana. Sekce Základní ochrana je rozdělena na Počítač a Web a e-mail. U obou se zobrazuje informace o stavu ochrany. Po jejich otevření se zobrazí pouze jednoduchý popis toho, co každá funkce přesně zajišťuje. V sekci Úplná ochrana jsou zobrazeny funkce, které nejsou ve verzi FREE dostupné a slouží tak pouze jako lákadlo pro zakoupení, vyšší, placené verze. Ve spodní části hlavní obrazovky je informace o posledním provedení kontroly, dále zvýrazněné tlačítko otestovat počítač a detaily o virové definici. Po kliknutí na otestovat se ihned spustí kontrola počítače. Pokud chce uživatel nastavit parametry kontroly nebo zvolit jiný typ testu, může kliknout na ozubené kolečko v pravé části tlačítka otestovat počítač. Je zde možné naplánovat test na vybranou dobu nebo vybrat z různých typů kontrol počítače. Kontroly jsou Test počítače, Hloubkový test, Test USB/DVD, Test souborů a složek, Test výkonu a Test po restartu. V záhlaví uživatelského prostředí se zobrazují dvě volby. První z nich je Moje AVG, kde si uživatel může doinstalovat různá rozšíření a další produkty od AVG. Druhou je Nabídka, která obsahuje možnosti nastavení programu, jeho podpory, nápovědy nebo informací o něm. V zápatí uživatelského prostředí je další z nabídek na zakoupení vyšší verze ochrany od vydavatele. Celkově vzhled působí příjemně, ovládací prvky jsou rozmístěné logicky a práce s programem je intuitivní. Nedostatkem je možná až přílišná reklama na placené produkty od výrobce.



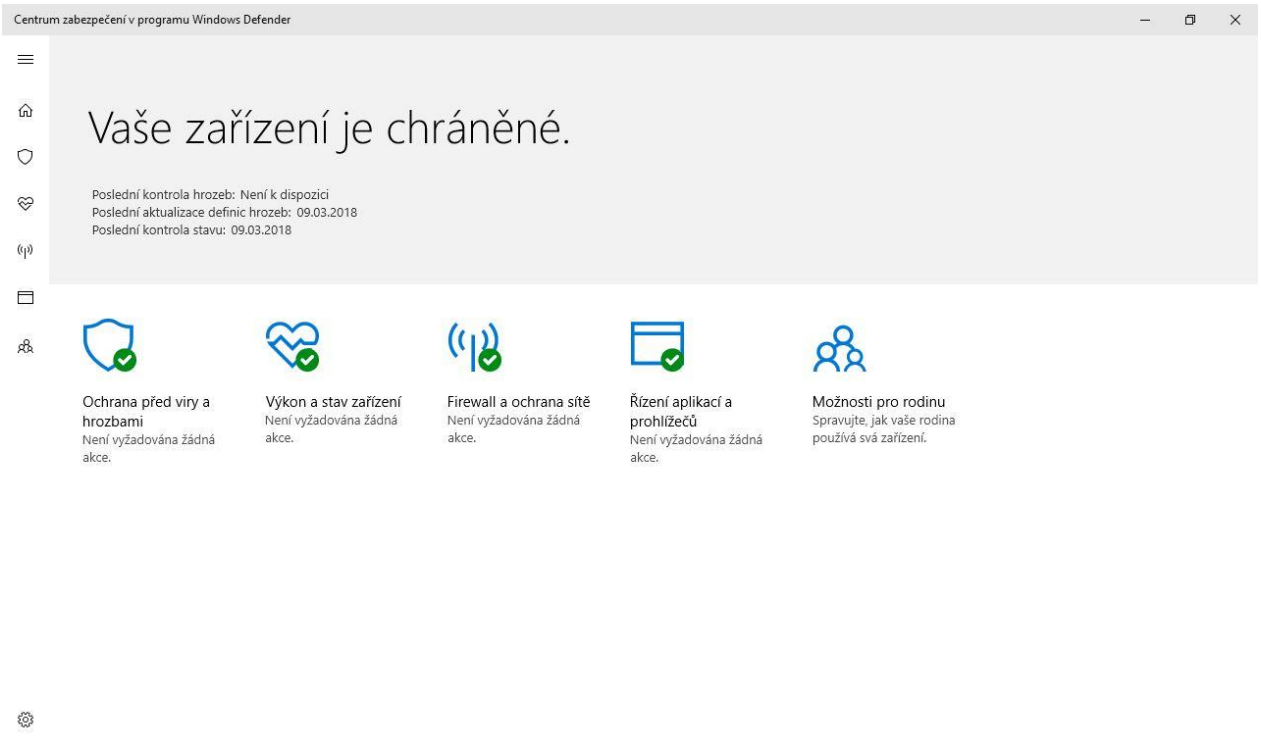
Obrázek 3: AVG AntiVirus Free – uživatelské rozhraní

4.2.4 Windows Defender

Tato antivirová ochrana je dodávaná přímo od společnosti Microsoft společně s operačním systémem Windows. Dříve se ve většině případů používal ve spojení s Microsoft Security Essentials. Od verze operačního systému Windows 8 je však již plnohodnotnou ochranou před bezpečnostními hrozbami a nahradil tak zmiňovaný Microsoft Security Essentials. Program je integrovaný přímo v operačním systému. Uživatel je tak chráněný od první chvíle, kdy spustí své zařízení. Testována byla verze 4.12.16299.15

Windows Defender je dostupný v češtině a v poslední době jeho uživatelské rozhraní prošlo menší úpravou. Na úvodní obrazovce Domů se zobrazuje základní přehled o stavu zařízení a datu, kdy došlo k poslední kontrole funkcí zařízení. Dále jsou zde v dolní části okna zastoupeny ikony všech funkcí, které program nabízí. Jsou jimi Ochrana před viry a hrozbami, Výkon a stav zařízení, Firewall a ochrana sítě, Řízení aplikací a prohlížečů a Možnosti pro rodinu. Na tyto funkce se dá dostat i z bočního menu, které je dostupné v levé části uživatelského rozhraní programu. Jako první z funkcí je nabízena

Ochrana před viry a hrozbami. V této sekci lze provést kontroly disku, a to Úplnou, Vlastní nebo Offline kontrolu. Pokud má uživatel nainstalovaný jiný antivirový software, je místo již jmenovaných kontrol zobrazen odkaz na otevření využívané ochrany. Další z nabízených funkcí je Výkon a stav zařízení, který kontroluje, zda je operační systém aktuální a jestli neexistují nějaké problémy s úložištěm, ovladači zařízení, případně životností baterie. Je také možnost provést čistou instalaci aktuálního systému Windows bez ztráty osobních souborů. V menu funkcí následuje Firewall a ochrana sítě. Zde můžete nalézt síťová připojení, nastavení Firewall, případně vyřešit problémy se sítí a internetem. Další z funkcí je Řízení aplikací a prohlížečů, kde si uživatel může nastavit filtr SmartScreen pro aplikace a internetové prohlížeče. Jako poslední lze využít Možnosti pro rodinu. Uživatel zde může nastavit rodičovskou kontrolu a zobrazit informace o zařízeních, která má přiřazena k uživatelskému účtu. Program má jednoduchý světlý vzhled a základní funkce ochrany. Některé prvky jsou méně srozumitelné, ale celkově se po krátkém seznámení s funkčností uživatel naučí program ovládat.



Obrázek 4: Windows Defender – uživatelské rozhraní

4.2.5 Bitdefender Internet Security

Antivirovou ochranu Bitdefender Internet Security vyvíjí rumunská společnost Bitdefender. Tu založil v roce 2001 Florin Talpeş, který je nyní jejím generálním ředitelem. Pro testování byla vybrána verze Internet Security se zkušební (trial) licencí na 30 dní. Vydavatel sice nabízí i antivirovou ochranu zdarma, ta však není dostupná v češtině. Testovaný program byl ve verzi 22.0.19.242.

Instalace trvala, oproti ostatním testovaným ochranám, delší dobu a její průvodce obsahoval několik gramatických chyb v českých příkazech. Před spuštěním programu se musí uživatel nejdříve registrovat. Uživatelské rozhraní je, podobně jako u některých konkurentů, kombinací tmavého pozadí se světlými ovládacími prvky. V levé části okna programu nalezneme ovládací panel, který obsahuje všechny důležité ovládací prvky. Hlavní obrazovkou rozhraní a první volbou v ovládacím panelu je Ochrana. Ta uživatele informuje o zabezpečení jeho zařízení, aktuálnosti software a umožňuje spouštět testy počítače, zobrazit a spustit funkce ochrany systému. Je zde také možné zapnout nebo vypnout tzv. autopilota. Autopilot dokáže potlačit oznámení o hrozbách a vyřešit je bez nutnosti uživatelského přičinění. V ovládacím panelu následuje volba Soukromí. Její obrazovka se v horní části shoduje s tou předchozí a liší se pouze v nabízených funkcích. Uživatel může využít správu hesel, šifrování připojení přes VPN, bezpečné placení na internetu a další. Třetím prvkem v ovládacím panelu jsou Nástroje. Ty slouží jako doplňky k antivirové ochraně. Bitdefender v menu dále nabízí Aktivitu, která zobrazuje statistiky ochrany aplikací, blokovaných hrozeb a útoků na zařízení. Upozornění se zobrazují jako další volba menu. Podává uživateli informace o hrozbách a doporučených akcích. V ovládacím panelu jsou na jeho konci umístěny Účet, Nastavení a Podpora. Jsou zde informace o účtu a licenci, nápověda k programu a nastavené celé antivirové ochrany. Bitdefender Internet Security obsahuje spoustu funkcí, nastavení a doplňků. Pro uživatele může být prostředí těžší na zorientování a ztěžuje tak jeho ovládání.

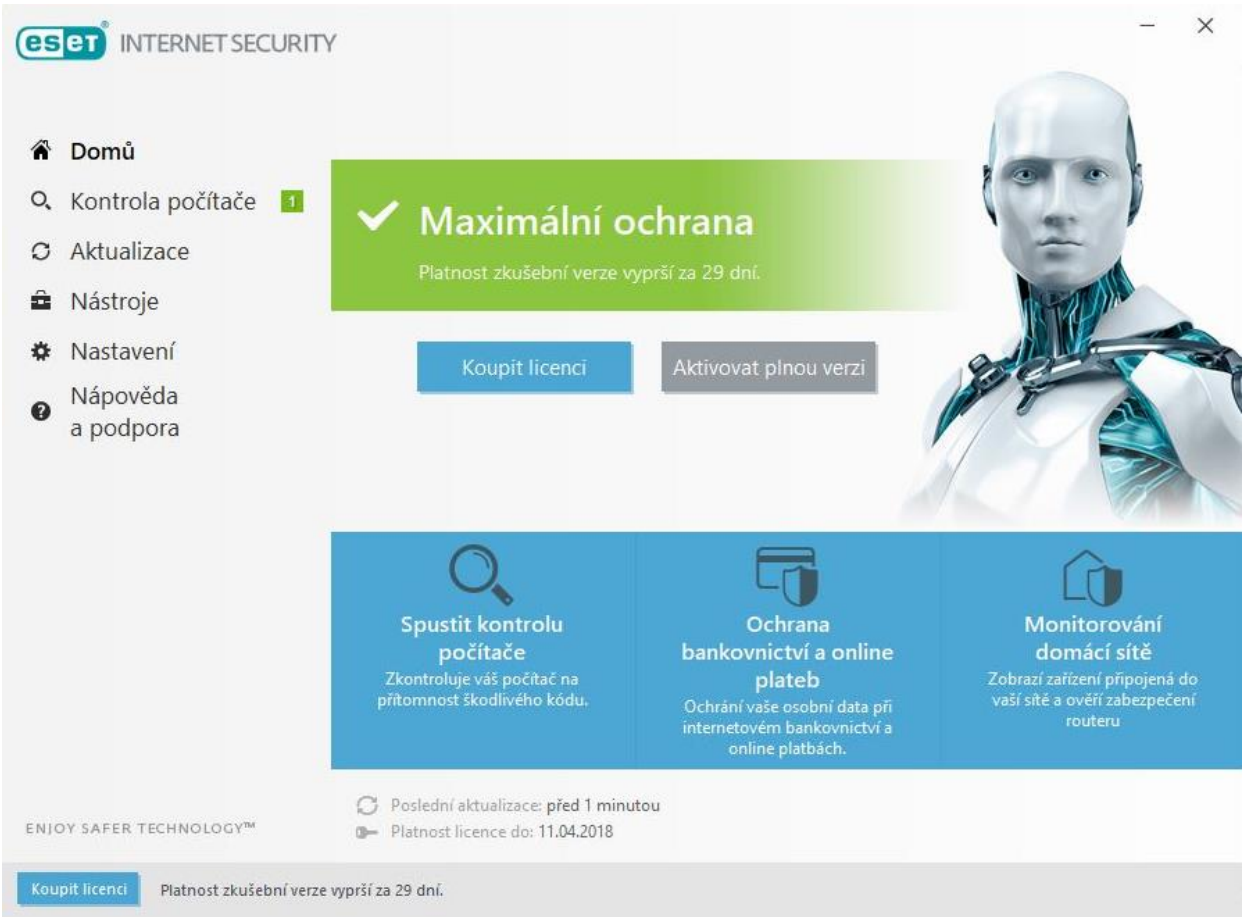
Obrázek 5: Bitdefender Internet Security – uživatelské rozhraní

4.2.6 Eset Internet Security

Eset Internet Security je antivirová ochrana od slovenské společnosti ESET spol. s.r.o. Ta byla založena v roce 1992 Miroslavem Trnkou a Peterem Paškem. Eset jako jediný z výrobců antivirů, které byly testovány, neposkytuje žádný z programů zdarma. Testována tak byla verze Internet Security se zkušební licencí na 30 dní. Program je samozřejmě dostupný v českém jazyce a měření probíhalo na verzi programu 11.0.159.9.

Průvodce instalací byl v češtině. Instalace samotná proběhla rychle. Pro spuštění není nutná registrace a je tak možné ochranu rovnou využívat. Celé uživatelské rozhraní je v barvách firemního loga, tedy v bílé, modré a šedivé. Informace a notifikace jsou v zelené barvě. Jako u většiny antivirových programů má ovládací panel na levé straně obrazovky. Na domovské obrazovce je pouze zpráva o zabezpečení zařízení, možnost okamžitého spuštění kontroly počítače, ochrany plateb a online bankovnictví nebo zmonitorování domácí sítě, do které je zařízení připojeno. V menu je jako druhá volba v pořadí Kontrola počítače. V ní uživatel může provést kontrolu všech lokálních disků nebo využít jednu z pokročilých kontrol. Mezi pokročilými kontrolami je uživatelem konfigurovatelná

kontrola zařízení, kontrola výměnných médií (USB, DVD, CD a další) nebo možnost opakování poslední provedené kontroly. Další z možných kontrol počítače je přesunutí souborů myší na označené místo a jejich následný test. Sekce Aktualizace, která v ovládacím panelu následuje, informuje o nainstalované verzi programu, jeho poslední aktualizaci a poslední kontrole aktualizace. V hlavním menu následuje volba Nástroje, která nabízí již zmiňovanou ochranu bankovnictví nebo monitoring sítě. Oproti domovské obrazovce zde přibyla funkce Anti-Theft. Ta chrání data v případě odcizení nebo ztráty zařízení a je i schopná podat informaci o jeho poloze. Poslední dvě funkce v levém ovládacím panelu jsou Nastavení a Nápověda a podpora. Jednou ze zajímavostí je, že si uživatel může importovat nastavení zabezpečení z jiného zařízení. Uživatelské prostředí je velice líbivé, intuitivní a snadno se s ním pracuje.



Obrázek 6: Eset Internet Security – uživatelské rozhraní

4.3 Výsledky měření

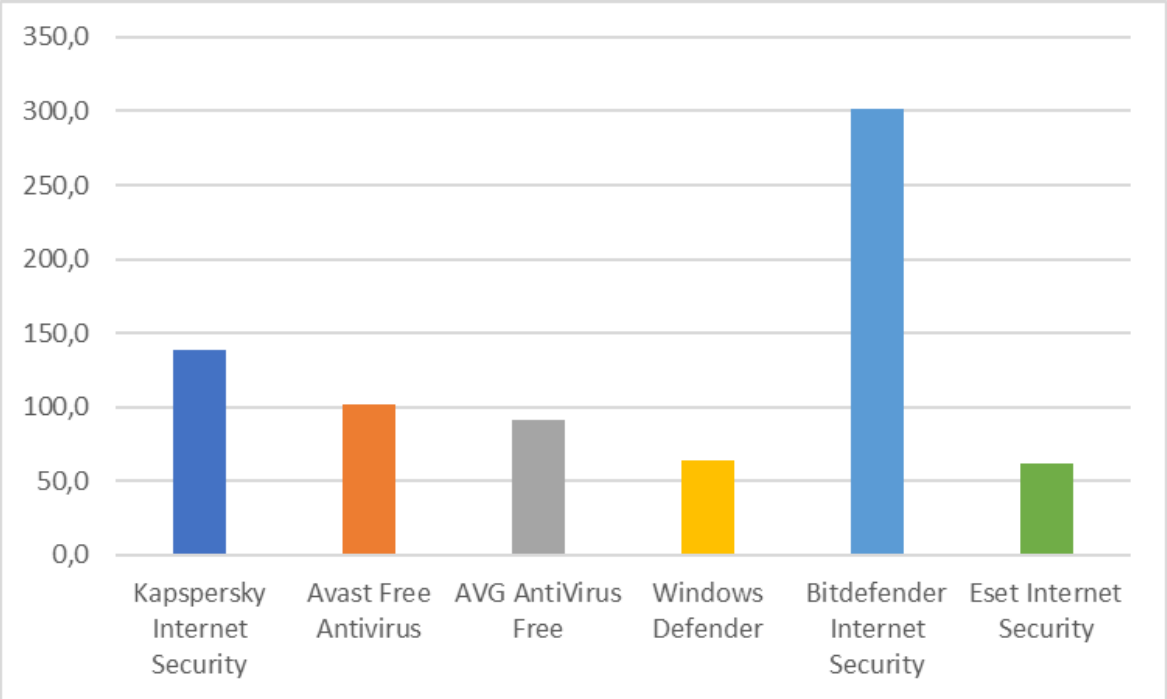
4.3.1 Využití RAM

Měření probíhalo při spuštěném antivirovém programu. Sledovalo se využití operační paměti všemi procesy, které měla testovaná ochrana spuštěné. Nejmenší zátěž na výkon z hlediska operační paměti měl Eset Internet Security (61,5 MB). O trochu více náročný byl Windows Defender s průměrnou zátěží 63,7 MB. Další v pořadí byly Avast, AVG a Kaspersky. S velkým odstupem dosáhl nejhoršího výsledku Bitdefender, který více než dvojnásobné využití RAM než v pořadí pátý Kaspersky.

Tabulka 3: Výsledky měření – využití RAM

Název antivirového programu	Využití RAM [v MB]			Průměrné využití RAM
Kapspersky Internet Security	135,3	139,8	139,7	138,3
Avast Free Antivirus	100,0	107,9	97,1	101,7
AVG AntiVirus Free	98,4	90,2	86,3	91,6
Windows Defender	64,2	62,0	65,0	63,7
Bitdefender Internet Security	306,4	298,8	299,3	301,5
Eset Internet Security	60,2	61,3	62,9	61,5

Graf 1: Výsledky měření – využití RAM



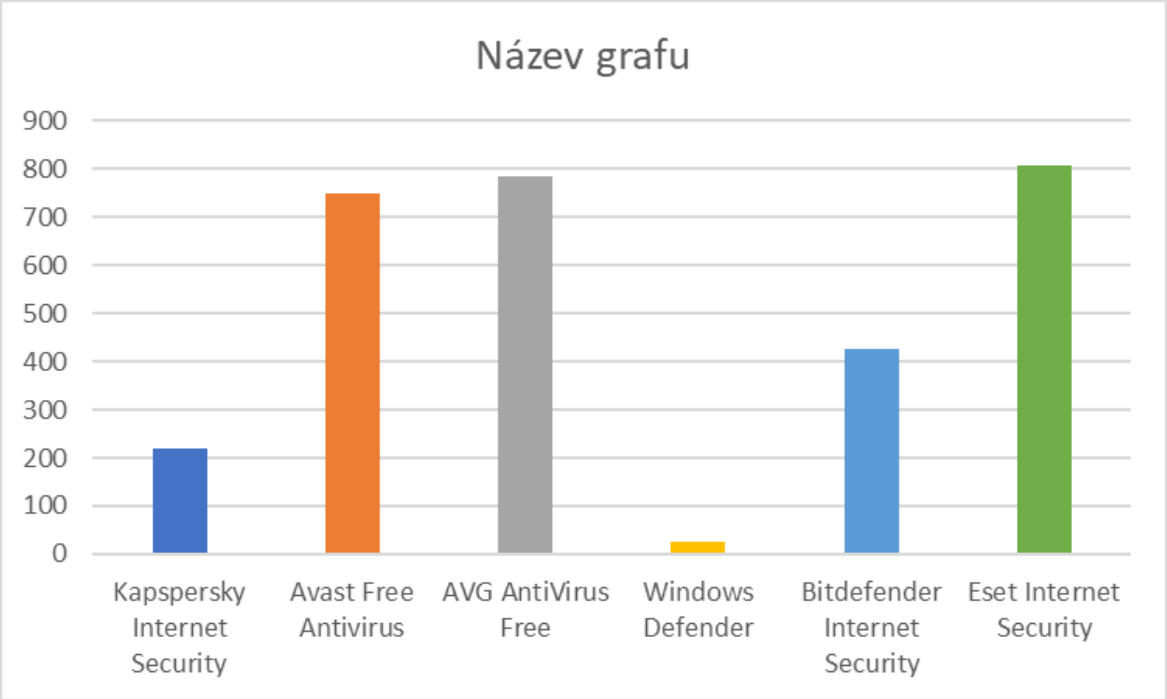
4.3.2 Zabraná kapacita na disku

Zabraná kapacita na disku spočívala v průzkumu disku, na kterém byl testovaný program nainstalovaný. Nejméně místa na disku zabíral s velkým odstupem Windows Defender (24 MB). Další programy už využívaly místo v řádech stovek MB. Kaspersky zabíral 220 MB a umístil se tak druhý v pořadí, následovaný Bitdefenderem s 424,9 MB. Dále je však velký skok k Avastu a AVG, které zabírali o více jak 300 MB kapacity disku. Největší náročnost na úložiště má však antivirová ochrana Eset a to 806 MB.

Tabulka 4: Výsledky měření – zabraná kapacita na disku

Název antivirového programu	Zabraná kapacita na disku [v MB]
Kapspersky Internet Security	220
Avast Free Antivirus	748
AVG AntiVirus Free	783
Windows Defender	24
Bitdefender Internet Security	424,9
Eset Internet Security	806

Graf 2: Výsledky měření – zabraná kapacita na disku



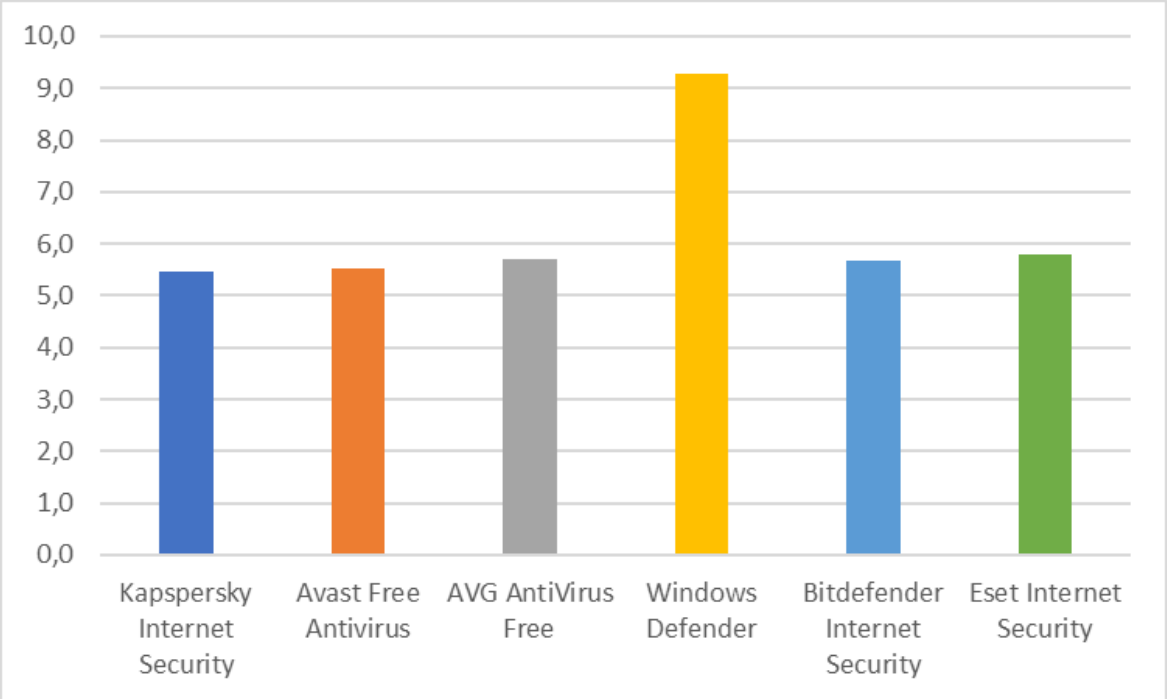
4.3.3 Vytížení CPU

Další z testů zaměřených na zatížení výpočetního výkonu zařízení, tentokrát procesoru. U každého antivirového programu proběhlo měření třikrát a výsledná hodnota se následně stanovila jako jejich aritmetický průměr. Hodnoty byly naměřeny v procentech. Kritérium je minimalizační, máme tdy zájem na co nejmenším využití procesoru. Nejhůře dopadl Windows Defender s 9,27% využití. Dále už je pořadí velmi vyrovnané. Eset s 5,80% následuje AVG s 5,70% a Bitdefender s 5,67%. Avast vytěžoval výkon procesoru z 5,53% a umístil se tak na druhém místě. Nejlépe v hodnocení tohoto kritéria tak s 5,47% skončil Kaspersky.

Tabulka 5: Výsledky měření – využití CPU

Název antivirového programu	Využití CPU [v %]			Průměrné využití CPU
Kaspersky Internet Security	5,2	5,4	5,8	5,47
Avast Free Antivirus	4,3	7,5	4,8	5,53
AVG AntiVirus Free	4,6	6,9	5,6	5,70
Windows Defender	10,1	9,2	8,5	9,27
Bitdefender Internet Security	5,8	5,2	6,0	5,67
Eset Internet Security	6,1	4,9	6,4	5,80

Graf 3: Výsledky měření – využití CPU



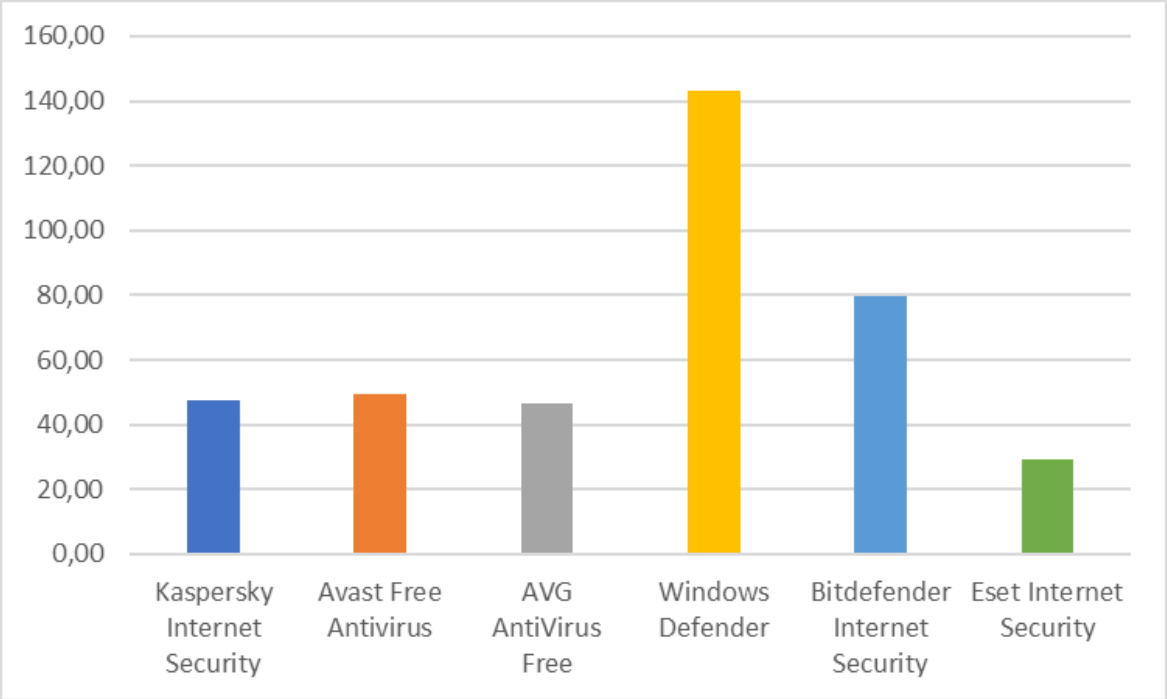
4.3.4 Rychlost kontroly disku

Kritérium hodnotilo průměrnou rychlost kontroly systémového disku, na kterém byla uložena všechna data. Nejrychleji zvládl kontrolu Eset Internet Security. Jeho průměrná kontrola disku trvala 29,02 minuty. Jako druhé v pořadí skončilo AVG těsně následované antivirovou ochranou od Kaspersky. V průměru o přibližně 30 minut déle trval test disku Bitdefenderem (79,62 minut). Absolutně nejhůře si v měření vedl Windows Defender, který testoval o více jak hodinu déle než druhý nejhorší Bitdefender.

Tabulka 6: Výsledky měření – rychlost kontroly disku

Název antivirového programu	Rychlost kontroly disku [v minutách]			Průměrná rychlost kontroly disku
Kaspersky Internet Security	51,42	45,23	46,50	47,72
Avast Free Antivirus	52,60	48,37	47,75	49,57
AVG AntiVirus Free	49,82	44,73	45,68	46,74
Windows Defender	143,17	140,50	145,70	143,12
Bitdefender Internet Security	80,82	79,30	78,75	79,62
Eset Internet Security	32,75	26,82	27,50	29,02

Graf 4: Výsledky měření – rychlost kontroly disku



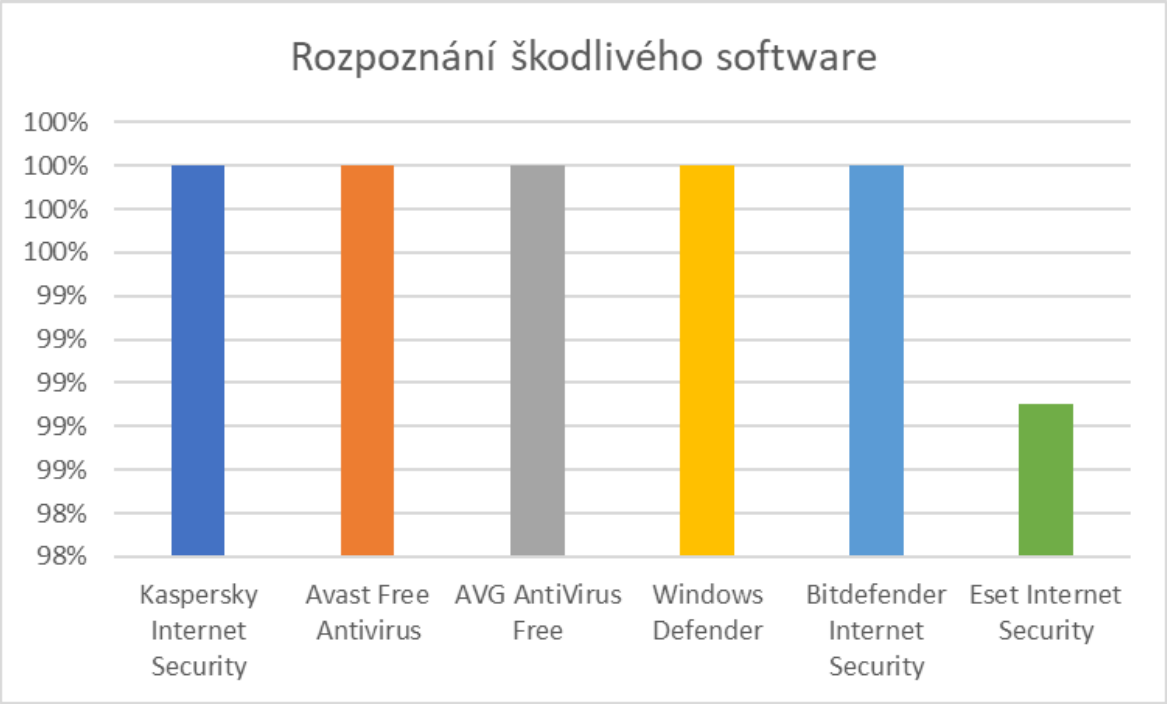
4.3.5 Schopnost rozpoznání škodlivého software

Výsledky tohoto testu vycházejí z měření profesionální nezávislé instituce AV-Test (zdroj). Ta se specializuje na oblast bezpečnosti informačních technologií. Publikované hodnoty testu jsou uváděné k prosinci roku 2017. Hodnoty úspěšnosti rozpoznání škodlivého software institut uvádí v procentech. Čím větší míra úspěšnosti rozpoznání škodlivého software, tím lépe. Z grafu jasně vyplývá nejhůře z testovaných antivirových programů Eset Internet Security. AV-Test naměřil úspěšnost rozpoznání škodlivého software 98,90%, což je dokonce méně než je průměrná hodnota úspěšnosti rozpoznání ze všech, institutem testovaných, antivirových programů. Průměrná úspěšnost činí 99,50%. Ostatní antivirové programy dosáhly na úspěšnost 100%. Konkrétně se jednalo o Avast, Avg, Kaspersky, Windows Defender a Bitdefender.

Tabulka 7: Výsledky měření – schopnost rozpoznání škodlivého software

Název antivirového programu	Míra rozpoznání škodlivého software
Kapspersky Internet Security	100 %
Avast Free Antivirus	100 %
AVG AntiVirus Free	100 %
Windows Defender	100 %
Bitdefender Internet Security	100 %
Eset Internet Security	98,9 %

Graf 5: Výsledky měření – schopnost rozpoznání škodlivého software



4.3.6 Množství falešných poplachů

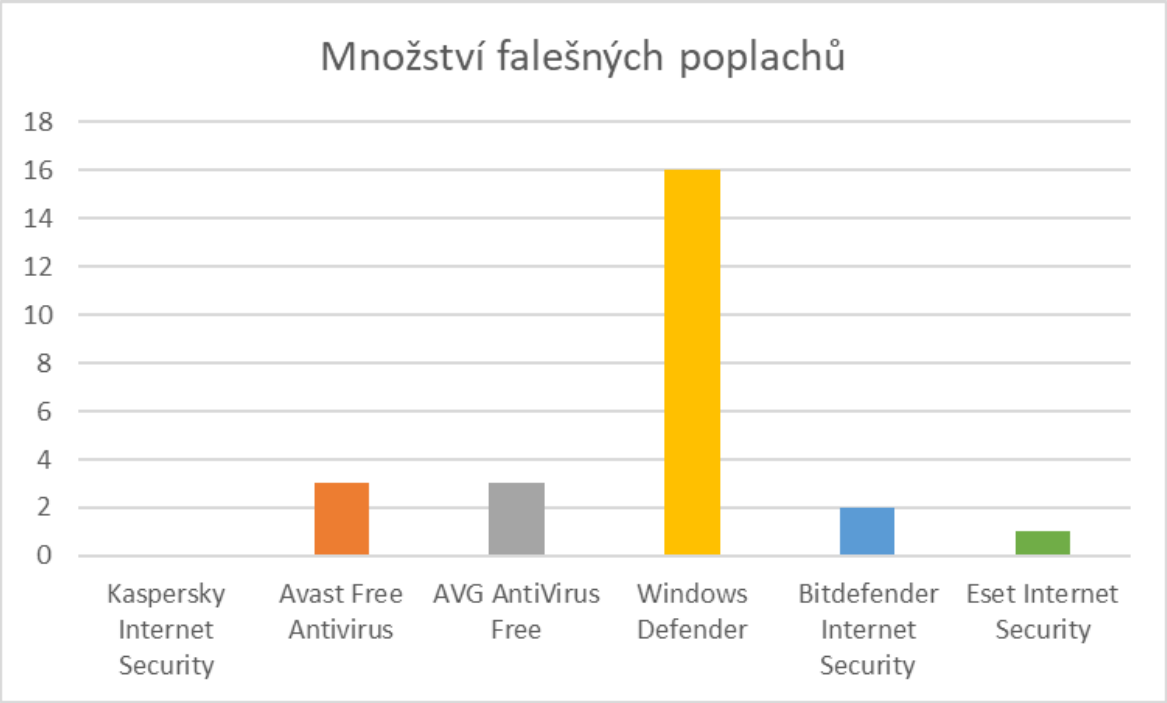
Data tohoto kritéria vycházejí, stejně jako míra úspěšnosti rozpoznání malware, z oficiálních zdrojů institutu AV-Test a jsou publikována k prosinci 2017. Toto měření spočívalo v zaznamenání případů, kdy antivirová ochrana chybně označí program nebo soubor jako škodlivý a pokusí se ho zablokovat, přičemž program nebo soubor je ve skutečnosti nezávadný. V tomto testu dopadl nejlépe antivirus Kapersky, u kterého nedošlo k žádnému falešnému poplachu. Pouze jednu falešnou detekci zjistil Eset a umístil se tak v tomto měření na druhém místě. Následuje Bitdefender se dvěmi a AVG s Avastem se třemi falešnými poplachy. S velkým odstupem si v tomto testu vedl nejhůře Windows Defender, u kterého bylo naměřeno 16 falešných poplachů.

Tabulka 8: Výsledky měření – množství falešných poplachů

Název antivirového programu	Počet falešných poplachů
Kapspersky Internet Security	0
Avast Free Antivirus	3
AVG AntiVirus Free	3
Windows Defender	16

Bitdefender Internet Security	2
Eset Internet Security	1

Graf 6: Výsledky měření – množství falešných poplachů



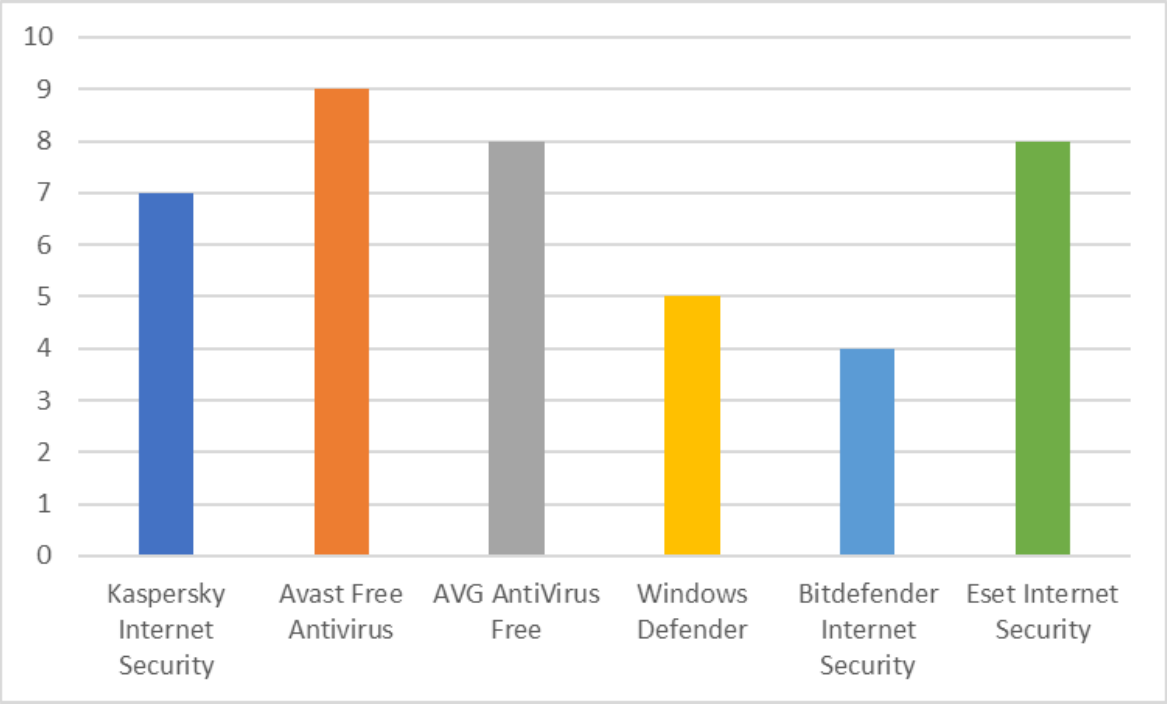
4.3.7 Uživatelské rozhraní

Hodnocení uživatelského rozhraní testovaných programů proběhlo seznámením s jejich funkcemi, ovládáním a prací s nimi. Každý antivirový software byl hodnocen za jeho vzhled a ovladatelnost. Pokaždé mohl získat od 0 do 5 bodů s celkovým možným ziskem až 10 bodů. Výsledná hodnota měřeného kritéria byla určena součtem získaných bodů za vzhled a ovladatelnost. Nejméně bodů získal Bitdefender Internet Security. Ten sice oplývá spoustou funkcí, které jsou ovšem zasazeny do nepřehledného uživatelského prostředí. Jeho ovladatelnost i vzhled taky byly hodnoceny nejhůře. O něco lépe si v ovladatelnosti vedl Windows Defender, který měl jednodušší vzhled a minimum funkcí. Kapersky Internet Security byl oproti zmiňovaným dobře ovladatelný a doplatil tak pouze na horší vzhled jeho prostředí. Na děleném druhém místě skončil s Eset Internet Security s AVG. Oba dosáhly stejného ohodnocení. Nejlépe si však vedl Avast, který na tom byl po vizuální stránce stejně jako AVG a Eset, ovšem ovladatelností předčil všechny testované programy.

Tabulka 9: Výsledky měření – uživatelské rozhraní

Název antivirového programu	Vzhled [max 5b]	Ovladatelnost [max 5b]	Celkový počet bodů
Kaspersky Internet Security	3	4	7
Avast Free Antivirus	4	5	9
AVG AntiVirus Free	4	4	8
Windows Defender	2	3	5
Bitdefender Internet Security	2	2	4
Eset Internet Security	4	4	8

Graf 7: Výsledky měření – uživatelské rozhraní



4.4 Výpočet Vícekriteriální analýzy variant

Pro výpočet vícekriteriální analýzy variant využiji metodu váženého součtu, která byla popsána v teoretické části této práce.

Nejdříve je třeba uvést souhrn výsledků jednotlivých měření, včetně popisu povah daných kritérií.

Tabulka 10: Vícekriteriální analýza variant – souhrn výsledků

Název	K1	K2	K3	K4	K5	K6	K7
Kaspersky Internet Security	138,27	220,00	5,47	47,72	0	6	7
Avast Free Antivirus	101,67	748,00	5,53	49,57	3	6	9
AVG AntiVirus Free	91,63	783,00	5,70	46,74	3	6	8
Windows Defender	63,73	24,00	9,27	143,12	16	6	5
Bitdefender Internet Security	301,50	424,90	5,67	79,62	2	6	4
Eset Internet Security	61,47	806,00	5,80	29,02	1	5	8
Povaha kritéria	MIN	MIN	MIN	MIN	MIN	MAX	MAX

Jak je z tabulky patrné, většina z nich je minimalizačního charakteru. Je tedy nutné všechna kritéria převést na maximalizační. Po převedení na stejný typ charakteru je možné určit jejich ideální Hj a bazální Dj variantu. Po provedení těchto kroků vyšla následující tabulka.

Tabulka 11: Vícekriteriální analýza variant – převod na stejný charakter kritérií

Název	K1	K2	K3	K4	K5	K6	K7
Kaspersky Internet Security	163,23	586,00	3,80	95,41	16,00	6,00	7,00
Avast Free Antivirus	199,83	58,00	3,73	93,55	13,00	6,00	9,00
AVG AntiVirus Free	209,87	23,00	3,57	96,38	13,00	6,00	8,00
Windows Defender	237,77	782,00	0,00	0,00	0,00	6,00	5,00
Bitdefender Internet Security	0,00	381,10	3,60	63,50	14,00	6,00	4,00
Eset Internet Security	240,03	0,00	3,47	114,10	15,00	5,00	8,00
Ideální varianta Hj	240,03	782,00	3,80	114,10	16,00	6,00	9,00
Bazální varianta Dj	0,00	0,00	0,00	0,00	0,00	5,00	4,00

Díky určení ideální a bazální varianty může být provedena normalizace. Výsledná tabulka normalizace je uvedena níže.

Tabulka 12: Vícekriteriální analýza variant – normalizace

Název	K1	K2	K3	K4	K5	K6	K7
Kaspersky Internet Security	0,68	0,75	1,00	0,84	1,00	1,00	0,60
Avast Free Antivirus	0,83	0,07	0,98	0,82	0,81	1,00	1,00
AVG AntiVirus Free	0,87	0,03	0,94	0,84	0,81	1,00	0,80
Windows Defender	0,99	1,00	0,00	0,00	0,00	1,00	0,20
Bitdefender Internet Security	0,00	0,49	0,95	0,56	0,88	1,00	0,00
Eset Internet Security	1,00	0,00	0,91	1,00	0,94	0,00	0,80
Váhy kritérií	0,26	0,05	0,14	0,07	0,03	0,39	0,06

V tabulce jsou nyní hodnoty v rozmezí od 0 do 1 pro zjištění užitku testovaných programů už tak stačí provést skalární součin vah kritérií s řádkem jednotlivých testovaných antivirových programů. Výsledná tabulka vícekriteriální analýzy je následující.

Tabulka 13: Výpočet vícekriteriální analýzy variant – výsledky

Název	Užitek
Kaspersky Internet Security	0,870
Avast Free Antivirus	0,886
AVG AntiVirus Free	0,878
Windows Defender	0,712
Bitdefender Internet Security	0,616
Eset Internet Security	0,530

5 Interpretace výsledků

Pomocí metody váženého součtu vícekriteriální analýzy variant bylo na základě vypočteného užitku určené pořadí testovaných programů:

1. Avast Free Antivirus
2. AVG Anti-Virus Free
3. Kaspersky Internet Security
4. Windows Defender
5. Bitdefender Internet Security
6. Eset Internet Security

Na prvním místě se umístil Avast Free Antivirus, který uspěl zejména v testech rozpoznání škodlivého softwaru a hodnocení uživatelského rozhraní. V ostatních měřeních sice nebyl nejlepší, ale držel se vždy v popředí.

Na druhém místě se umístil AVG Anti-Virus Free a těsně za ním Kaspersky Internet Security. AVG bylo oproti antiviru od Kaspersky lepší ve využití operační paměti, rychlosti kontroly disku a rozhraní. Kaspersky naopak dopadl lépe ve využití procesoru, množství falešných poplachů a využití místa v úložišti.

Jako čtvrtý se umístil překvapivě Windows Defender, který byl nejlepší v měření využité kapacity disku a druhý nejlepší ve využití operační paměti. Na předposledním místě skončil Bitdefender Internet Security, který měl sice největší využití RAM, ale v testu rozpoznání hrozeb byl stoprocentní.

Na posledním místě se uístil Eset Internet Security a to i přes nejlepší výsledky v testu využití RAM a rychlosti kontroly disku. Na vině je úspěšnost rozpoznání škodlivého software. Eset jako jediný nebyl 100% úspěšný, dosáhl pouze na 98,9%.

Jako nejlepší volba dle výsledků srovnávání antivirových programů vyšel pro českého uživatele Avast Free Antivirus.

6 Závěr

Ve své bakalářské práci jsem podrobně popsal bezpečnostní rizika, před kterými nás antivirové programy mají chránit. Doporučil jsem preventivní opatření proti těmto hrozbám a popsal metody jejich detekce. Vybrané programy jsem srovnal pomocí jejich testování na využití operační paměti, zabranou kapacitu v úložišti, využití procesoru, dobu kontroly disku, množství falešných poplachů, rozpoznání škodlivého software a uživatelské rozhraní. Zhodnocení jsem provedl metodou váženého součtu vícekriteriální analýzy variant.

I když jsou bezpečnostní hrozby všudypřítomné a nevyzpytatelné, na českém trhu jsou dostupné stále se zlepšující programy pro ochranu dat. Touto prací jsem dospěl k závěru, že nejvhodnější volbou pro českého uživatele je Avast Free Antivirus.

7 Seznam použitých zdrojů

[1] What is malware (malicious software)?. TechTarget [online]. Margaret Rouse, 2016 [cit. 2018-01-19]. Dostupné z: http://searchsecurity.techtarget.com/definition/malware

[2] Malware a Spyware. Počítačové viry [online]. 2018 [cit. 2018-01-19]. Dostupné z: http://www.viry.estranky.cz/clanky/malware-a-spyware.html

[3] Prevence před útokem. Viry.cz [online]. 2012 [cit. 2018-01-20]. Dostupné z: https://www.viry.cz/prevence-pred-utokem/

[4] Jak ochránit počítač před viry a zcizením dat. Dsl.cz [online]. 2018 [cit. 2018-01-20]. Dostupné z: http://www.dsl.cz/jak-na-to/jak-se-chranit-pred-viry

[5] Prevent virus or malware infection. Microsoft [online]. 2018 [cit. 2018-01-20]. Dostupné z: https://www.microsoft.com/en-us/wdsi/help/prevent-malware-infection

[6] What is spyware?. TechTarget [online]. Margaret Rouse, 2016 [cit. 2018-01-19]. Dostupné z: http://searchsecurity.techtarget.com/definition/spyware

[7] What is worm?. TechTarget [online]. Margaret Rouse, 2017 [cit. 2018-01-20]. Dostupné z: http://searchsecurity.techtarget.com/definition/worm

[8] What is virus (computer virus)?. TechTarget [online]. Margaret Rouse, 2016 [cit. 2018-01-19]. Dostupné z: http://searchsecurity.techtarget.com/definition/virus

[9] Počítačový vir. Počítačové viry [online]. 2017 [cit. 2018-01-19]. Dostupné z: http://www.viry.estranky.cz/clanky/pocitacovy-vir.html

[10] What is ransomware?. TechTarget [online]. Margaret Rouse, 2017 [cit. 2018-01-20]. Dostupné z: http://searchsecurity.techtarget.com/definition/ransomware

[11] Po světě se šíří nový ransomware. Technet.cz [online]. Roman Všetečka, Pavel Kasík, 2017 [cit. 2018-01-20]. Dostupné z: https://technet.idnes.cz/ransomware-wannacry-wcry-wanncrypt0r-ransomware-f7q-/sw_internet.aspx?c=A170513_070537_sw_internet_vse

[12] Kybernetický útok zasáhl přes 70 zemí. Idnes.cz [online]. Idnes.cz, 2017 [cit. 2018-01-20]. Dostupné z:https://zpravy.idnes.cz/kyberneticky-utok-anglie-narodni-zdravotnicka-sluzba-ppo-/zahranicni.aspx?c=A170512_214354_zahranicni_ale

[13] What is rootkit?. TechTarget [online]. Margaret Rouse, 2008 [cit. 2018-02-05]. Dostupné z: http://searchmidmarketsecurity.techtarget.com/definition/rootkit

[14] Co je to rootkit a jak ho odstranit. Avast [online]. [cit. 2018-02-05]. Dostupné z: https://www.avast.com/cs-cz/c-rootkit

[15] What is backdoor (computing)?. TechTarget [online]. Margaret Rouse, 2017 [cit. 2018-02-05]. Dostupné z: http://searchsecurity.techtarget.com/definition/back-door
[16] What is spam?. Webopedia [online]. Vangie Beal, [cit. 2018-02-05]. Dostupné z: https://www.webopedia.com/TERM/S/spam.html
[17] What is phishing?. TechTarget [online]. Margaret Rouse, 2017 [cit. 2018-02-05]. Dostupné z: http://searchsecurity.techtarget.com/definition/phishing
[18] Sociální inženýrství. Počítačové viry, 2017 [cit. 2018-02-05]. Dostupné z: http://www.viry.estranky.cz/clanky/socialni-inzenyrstvi.html
[19] How antivirus software works: Virus detection techniques. TechTarget [online].Lenny Zeltser, 2011 [cit. 2018-02-05]. Dostupné z: http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques
[20] Infection spreading through usb peripherals. USB fix [online]. 2015 [cit. 2018-02-05]. Dostupné z: https://www.usb-antivirus.com/2014/03/infections-spreading-usb-peripherals/
[21] Viry a počítače. Peetko [online]. 2017 [cit. 2018-05-02]. Dostupné z: http://www.peetko.estranky.cz/clanky/kontrola-integrity.html
[22] ŠUBRT, Tomáš et al. Ekonomicko-matematické metody. 2. vyd. Plzeň: Aleš Čeněk, 2015. 331 s. ISBN 978-80-7380-563-0.