

**ВЪТРЕШНИ ПРАВИЛА  
ЗА РАБОТА С АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА, В  
КОЯТО СЕ СЪЗДАВА, ОБРАБОТВА И СЪХРАНЯВА КЛАСИФИЦИРАНА  
ИНФОРМАЦИЯ НА ОРГАНИЗАЦИОННАТА ЕДИНИЦА „ВЪРХОВЕН  
АДМИНИСТРАТИВЕН СЪД“**

**Раздел I  
ОБЩИ ПОЛОЖЕНИЯ**

**Чл. 1.** (1) Тези правила се създават на основание чл. 47 от Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва и съхранява класифицирана информация (НЗОУСАИСМ).

Вътрешните правила се отнасят единствено за информацията, класифицирана като държавна или служебна тайна. С тях се определят правата и задълженията на потребителите на автоматизирана информационна система (АИС), в която се създава, обработва и съхранява класифицирана информация.

(2) Неспазването на вътрешните правила е основание за налагане на дисциплинарно наказание, както и за търсене на друга отговорност, в съответствие с нормативната уредба.

**Чл. 2.** Автоматизираната информационна система, в която се създава, обработва и съхранява класифицирана информация, наричана по-нататък АИС „ВАС“, е предназначена да осигури защитени информационни услуги на организационната единица.

**Чл. 3.** (1) АИС „ВАС“ се състои от самостоятелна компютърна конфигурация, свързана с принтер и от самостоятелни компютри без принтер, общо наричани по-нататък базови станции.

(3) Разпределението и използването на базовите станции се съгласува със служителя по сигурността на информацията и ръководителя на Organa по развитие и експлоатация (ОРЕ).

**Раздел II  
ФИЗИЧЕСКА, ПЕРСОНАЛНА И ДОКУМЕНТАЛНА СИГУРНОСТ**

**Чл. 4.** (1) АИС „ВАС“ не е свързана с локалната мрежа на съда, интернет и други публични електронни и комуникационни мрежи и е разположена в зони за сигурност, клас I и клас II, в изпълнение на чл. 43(1) от НЗОУСАИСМ.

(2) Физическият достъп до зоните за сигурност клас I и клас II е ограничен до определените длъжностни лица, при осигурен контрол на достъп. Системата за контрол на физическия достъп включва използването на пропускателен режим, сигнално-охранителна техника, визуално наблюдение.

**Чл. 5.** Достъпът до ресурсите на АИС „ВАС“ е ограничен само до лица, имащи разрешение за достъп до класифицирана информация с ниво не по-ниско от „Секретно“, при спазване на принципа „необходимост да се знае“. В организационната единица това са всички магистрати, които

съгласно чл. 39, ал. 3, т. 3 от ЗЗКИ получават, считано от момента на встъпването им в длъжност, право на достъп до всички нива на класифицирана информация за срока на заемане на длъжността им при спазване на принципа „необходимост да се знае“ (само за конкретното дело), и служителите, притежаващи разрешение за достъп за работа с класифицирана информация с ниво „Секретно“ или по-високо.

**Чл. 6.** Всички документи, съдържащи класифицирана информация, които се създават, обработват и съхраняват в АИС „ВАС“, се идентифицират, маркират и контролират по подходящи начини, като маркировката на документите осигурява еднозначна информация за нивото на класификация при работа с тях.

**Чл. 7.** Потребителите на АИС биват:

1. Потребители с директен достъп - системен персонал, отговарящ за експлоатацията, развитието, управлението или сигурността и потребители, работещи със съответните приложения и програми на АИС;

2. Потребители с индиректен достъп - които използват материални носители на класифицирана информация – флаш памети за съхраняване на информация, обработена от АИС.

**Чл. 8.** (1) Материалните носители за съхранение на класифицирана информация до ниво „Секретно“ – флаш памети, се маркират, регистрират и съхраняват в регистратурата за класифицирана информация на организационната единица. Те се завеждат персонално на конкретния потребител и той ги получава за текущо използване срещу подпис, като носи изцяло отговорността за тяхното опазване и съхранение до връщането им в регистратурата.

(2) Материалните носители за съхранение на класифицирана информация до ниво „Секретно“ – флаш памети се използват единствено и само с базовите станции, част от АИС. Забранено е да се използват тези носители с други компютри.

(3) Потребителите, които нямат създадени потребителски профили на базовите станции, но имат заведени персонално флаш памети, могат да ги използват само за съхраняване на класифицирана информация до ниво „Секретно“. Самата класифицирана информация се обработва на базовите станции, част от АИС „ВАС“.

**Чл. 9.** Регистрирането, маркирането, контролът и унищожаването на материалните носители на многократен запис на класифицирана информация, се извършват по реда на глава V, раздел XII от ППЗЗКИ. Информацията и материалите, които вече не се използват за осигуряване на достъп до ресурсите на АИС „ВАС“, се унищожават по начин, недопускащ възстановяване на информацията.

**Чл. 10.** Правомощията на персонала, работещ с АИС „ВАС“ са определени така, че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи от сигурността на АИС.

**Чл. 11.** Потребителите преминават обучение по сигурността на АИС „ВАС“ съгласно чл. 47 от НЗОУСАИСМ и подписват декларация по образец - **Приложение № 2**, че са запознати и ще спазват настоящите Вътрешни правила. При успешно завършило обучение те се допускат до работа в АИС „ВАС“.

### **Раздел III ПРАВА И ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ НА АИС „ВАС“**

**Чл. 12.** (1) Всеки потребител на АИС има право да ползва единствено тази базова станция, за която е получил право на достъп чрез потребителско име и парола, предоставени му от администратора по сигурността на АИС и за цели, пряко свързани с дейността и служебните му задължения.

(2) Потребителите изпълняват указанията на администратора по сигурността на АИС, свързани със сигурността на системата. Потребителите уведомяват администратора по сигурността на АИС за случаи или съмнения за компрометиране на сигурността.

**Чл. 13.** (1) Съгласно чл. 62 от НЗОУСАИСМ за всеки потребител на АИС се създава потребителски профил, включващ валидно потребителско име и първоначална парола, осигуряващ му еднозначна идентификация и автентификация, които предхождат всички останали негови действия.

(2) Осъществява се контрол на достъпа по преценка - осигуряване на достъпа до обектите на АИС чрез предоставяне на права за достъп на базата на идентификацията на потребителя или неговата принадлежност към потребителска група; правата за достъп се предоставят само от упълномощени потребители или от администратора по сигурността на АИС на организационната единица (ОЕ); механизмите за контрол осигуряват възможност за разделяне на потребителите и за достъп до информацията според принципа "необходимост да се знае".

(3) При първото си влизане в базовата станция, потребителят е длъжен незабавно да смени първоначалната си парола за достъп, определена от администратора по сигурността, съгласно изискванията, описани в **Приложение № 1**.

**Чл. 14.** Всеки потребител използва само предоставеното му потребителско име и лична парола и е длъжен да ги съхранява на сигурно място. Парола, станала известна на неоторизирано лице, трябва да се смени незабавно. Отговорност за смяната на паролата носи изцяло потребителят – вж. **Приложение № 1**.

**Чл. 15.** За съхраняване и защита на класифицираната информация в АИС, на всяка базова станция е създадена персонална поименна папка „Документи“ за всеки потребител, в която само той има достъп за четене и писане. Препратка до тази папка е поставена на екрана на потребителя, в профила му. Потребителят има право да работи и записва информацията си само в нея.

**Чл. 16.** Разпечатването на материали, съдържащи класифицирана информация, при работа на самостоятелните компютри – базови станции, които са без принтер, става, като материалът бъде съхранен на персонално заведената в регистратурата за класифицирана информация флаш памет. След това документът трябва да бъде отворен от самостоятелната компютърна конфигурация, намираща се в регистратурата за класифицирана информация и разпечатан на принтера, свързан към нея.

**Чл. 17.** (1) Всеки потребител е отговорен за действията, извършени в компютърната среда на АИС „ВАС“ с неговото потребителско име и парола, когато това се дължи на виновното му поведение или на бездействието му.

(2) Чрез системните средства на операционната система се води непрекъснат запис на събития, свързани със сигурността на АИС (одитни записи); записват се всички действия, свързани с контрола на достъпа, включително неуспешни опити за достъп, създаване или разрушаване на обекти или действия на оторизирани субекти, влияещи на сигурността на информационната система; осигурена е възможност за изучаване на одитните записи и установяване на свързаните със сигурността действия на отделните субекти на АИС.

**Чл. 18.** Всеки потребител е длъжен да ползва АИС с грижата на добър стопанин и да спазва следните правила за експлоатация:

1. да не премества базовите станции от определените им места;  
2. да не поставя книги, хартия, дрехи, хранителни продукти, напитки и други предмети в близост до базовите станции и върху тях, с оглед нормалното им охлаждане;

3. да поддържа базовите станции чисти, като за почистване не трябва да се използват спирт и други агресивни препарати, които могат да повредят повърхностите; за целта може да се използва леко навлажнена мека кърпа, след като устройствата се изключат от електрическото захранване;

4. да не допуска попадане на чужди тела и течности в базовите станции. При възникване на инцидент или повреда, потребителят веднага трябва да изключи устройството от електрическото захранване и да уведоми незабавно администратора на АИС;

5. да не допуска прегъване, опъване, притискане и стъпване върху свързващите кабели;

6. да не ограничава по никакъв начин работата на софтуера за управление на базовите станции и антивирусната защита.

**Чл. 19.** Потребителят няма право:

1. да отваря и променя конфигурацията на базовата станция, монитора и принтера;

2. да изключва свързващите кабели при прекъсване на работния процес;

3. да променя настройките в хардуерния SETUP на компютъра (BIOS), системните настройки на операционната система, потребителския интерфейс и конфигурацията на компютъра;

4. да инсталира или позволява на друго лице инсталирането на софтуер и хардуер на компютъра;

5. да предоставя на друго лице своето потребителско име и парола.

## **Раздел IV ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ**

**§ 1.** Приложенията се актуализират при необходимост. Настоящите Правила и актуалната версия на приложенията се публикуват във ведомствената информационна система, в раздел "Заповеди" – „Работа с класифицирана информация“.

**§ 2.** Контролът по работата с АИС и обучението на персонала, се извършва от ОРЕ, администратора по сигурността на АИС и от администратора на АИС.

## **ПРАВИЛА**

### **за използване на потребителските имена и пароли в АИС „ВАС**

#### **1. Създаване на потребителски акаунт (потребителско име и парола)**

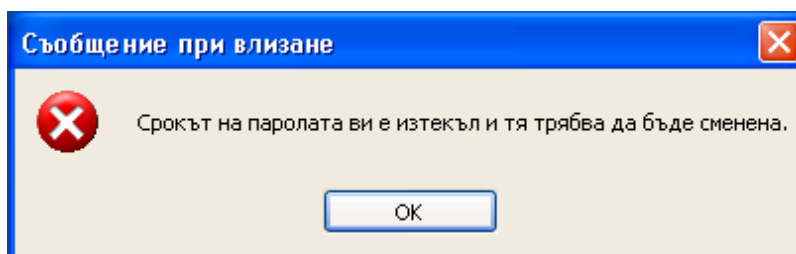
1.1. За всеки потребител на АИС се създава потребителски профил, включващ валидно потребителско име и първоначална парола, осигуряващ му еднозначна идентификация и автентификация, като и достъп до ресурсите на АИС. Тези данни се предоставят на потребителя от администратора по сигурността на АИС в непрозрачен запечатан плик. При първото си влизане чрез дадените му идентификационни данни, потребителят е задължен да промени паролата си за достъп и да постави своя парола, за съхранението на която той отговаря.

#### **2. Промяна на паролата от потребителя**

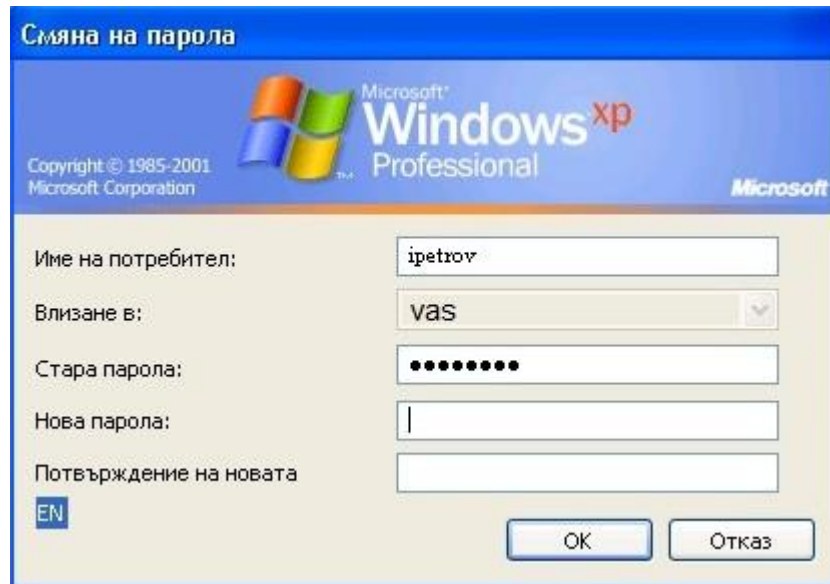
2.1. За гарантиране на информационна сигурност и защитеност на данните, на всеки 90 дена потребителят трябва да променя своята парола, за което излиза системно съобщение на екрана на компютъра.

#### **2.2. Указания за смяна на паролата**

На всеки 90 дена, компютърът автоматично издава съобщение за смяна на паролата. Трябва да се натисне бутонът "ОК".



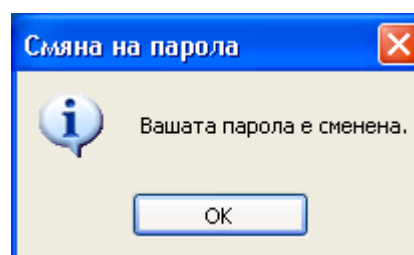
В полето "Стара парола" се изписва старата парола. В полетата "Нова парола" и "Потвърждение на новата" се въвежда новата парола. Повторното въвеждане на новата парола е за да се избегнат евентуални грешки при изписването. Необходимо е да се обръща внимание на езика и регистъра на буквите, с които се въвежда паролата.



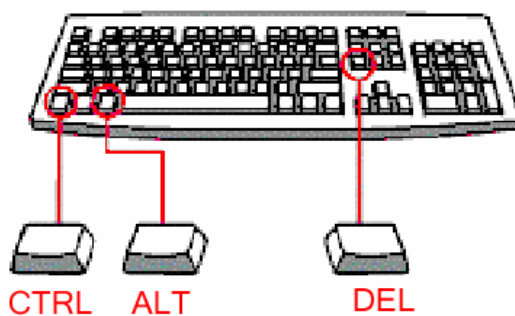
Новата парола трябва да се различава от старата, да съдържа минимум 8 символа (букви и цифри) и да не повтаря 5 предишни пароли. След попълване на данните, се натиска бутонът "OK".



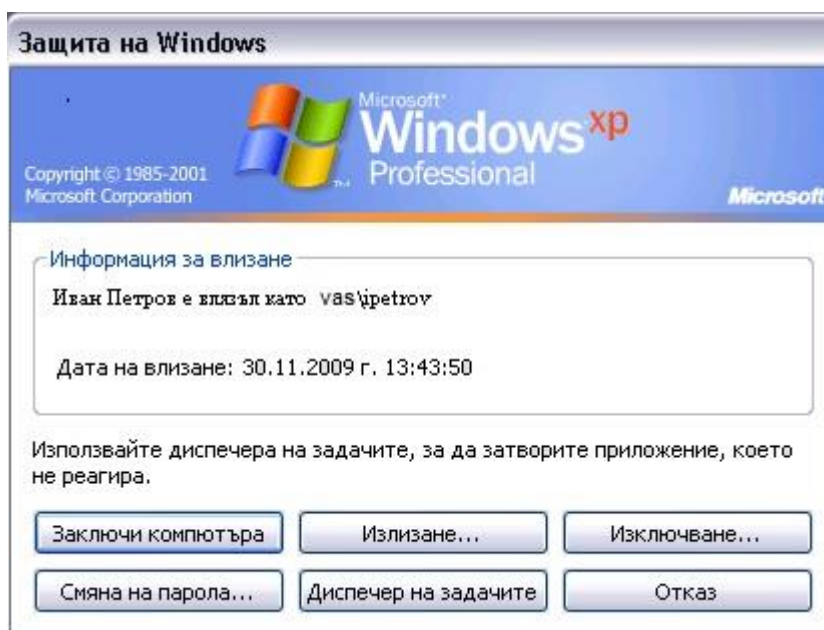
При успешна смяна на паролата се появява потвърждение, че паролата е сменена успешно.



2.3. Указания за смяна на паролата по желание на потребителя  
Потребителската парола може да се сменя по всяко време чрез едновременното натискане на клавишната комбинация:



На екрана се появява следният прозорец:

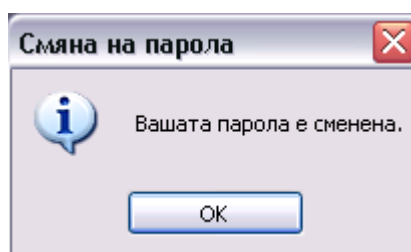


Натиска се бутонът "Смяна на парола". Появява се прозорец, аналогичен на описания по-горе, където по същия начин трябва да се въведе в съответните полета старата парола, новата парола и да се натисне бутонът "ОК".





Отново се получава потвърждение за успешно сменена парола.



2.4. Съвети за успешно извършване на смяната на паролата и за подобряване на сигурността

- Да се използват разнообразни символи – добрата парола включва в себе си малки и главни букви, цифри и символи: !@#\$%^&<>:; ;

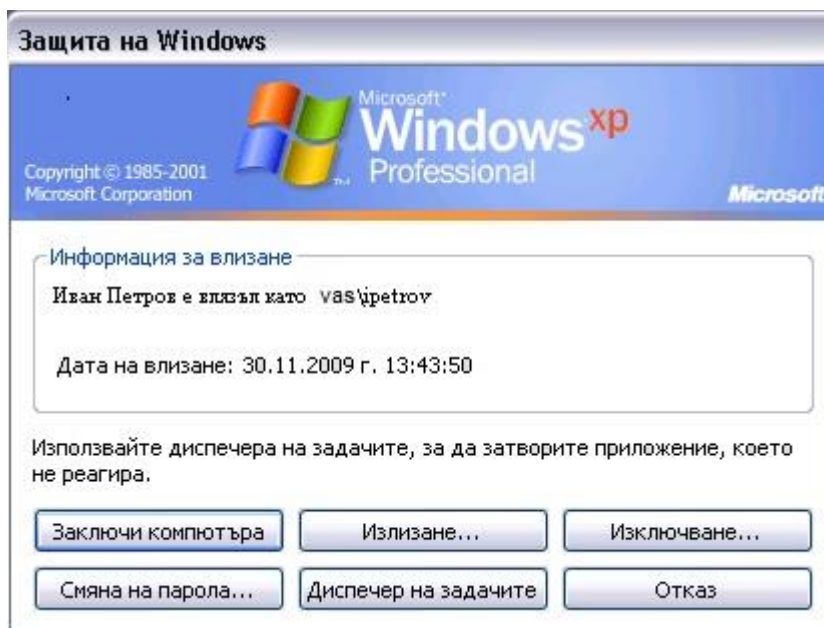
- Дължина – колкото по-дълга е, толкова по-добре. Минималната дължина е 8 символа.

- Семантика – от гледна точка на по-лесното запомняне, често паролите описват нещо от обкръжаващата среда. За съжаление, това е лоша практика, от която се възползват недоброжелателни индивиди, имащи интерес да разберат паролата. За да бъдат затруднени максимално, добре е да не се използват речникови думи от който и да е език, особено английски и български, производни на потребителското име (*idraganov - idr@gan0v*), лични данни или характеристики: име на съпруг/а, домашен любимец, деца, рождена дата, ЕГН и др. подобни. Не се препоръчват и елементарни клавиатурни последователности от типа "qwerty", "zxcvbnm", и особено "12345". Не следва да се използват реверсирани думи: *parola - alorap*.

- Паролите са лични и не трябва да се споделят с никого. Потребителят на АИС отговаря за съхранението и опазването на паролата си. При съмнение за компрометиране на сигурността на паролата, незабавно следва да бъде уведомен администраторът по сигурността на АИС или администраторът на АИС. При 5 поредни опита за влизане с погрешно изписана парола, достъпът на потребителя се блокира.

2.5. Допълнителни указания

В случай на кратко отсъствие на потребителя от работното му място на базовата станция, препоръчително е да се заключва компютърът – чрез едновременно натискане на клавишите Ctrl-Alt-Del и след това на бутона “Заключи компютъра”.



За да се влезе отново в компютъра, едновременно се натискат клавишите Ctrl-Alt-Del и след това се изписва потребителското име и паролата. При необходимост от по-продължително отсъствие на потребителя от работното му място е препоръчително да се изключва компютърът.

**Приложение по чл. 47 от НЗОУСАИСМ**

**ДЕКЛАРАЦИЯ**

Долуподписаният(ата),

.....  
(име, презиме и фамилия)

на  
длъжност.....  
във ВАС",

**ДЕКЛАРИРАМ:**

Запознат(а) съм с Вътрешните правила за работа с АИС „ВАС“, в която се създава, обработва и съхранява класифицирана информация, като се задължавам да спазвам всички правила, указания, процедури и свързаните с тях права, задължения и ограничения и ще опазвам същата до изтичането на сроковете за защитата ѝ по чл. 34 от ЗЗКИ.

Дата: .....  
.....

Декларатор:  
  
(подпис)