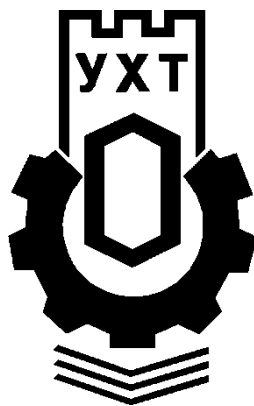


**УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ –  
ПЛОВДИВ**



**П Р А В И Л Н И К**

**ЗА ОСИГУРЯВАНЕ НА ДОСТЪП И РАБОТА  
С ИНФОРМАЦИОННИ ПРОДУКТИ В УХТ**

**ПЛОВДИВ**

**2017 г.**

# **УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ – ПЛОВДИВ**

**УТВЪРДИЛ,**

**РЕКТОР: П**

/проф. д.т.н. инж. К. Динков/

## **ПРАВИЛНИК**

### **ЗА ОСИГУРЯВАНЕ НА ДОСТЪП И РАБОТА С ИНФОРМАЦИОННИ ПРОДУКТИ В УХТ**

#### **РАЗДЕЛ I**

##### **Основни положения**

**Чл. 1.** Този правилник урежда реда и условията за осигуряване на достъп и работа с информационни продукти в Университета по хранителни технологии (УХТ) – Пловдив.

**Чл. 2.** (1) В УХТ съществува университетска информационна и комуникационна инфраструктура, която включва:

1. информационни ресурси, включително архив, Уеб сървъри, информационни източници, базирани в локални мрежи, специализирани бази данни, файлове на потребители и др.;
2. информационни системи с различно предназначение;
3. опорна компютърна мрежа;
4. компютърни зали и др.

(2) Процесите на интеграция на информационни системи и масиви се извършва на основата на научно обосновани стандарти и нормативна база за обучение, изследвания, управление и оценка на академичното качество.

(3) Сектор „Информационни технологии и комуникации“ към „Център за проектна и информационна дейност” е специализирано звено, което администрира и участва в планирането, изграждането, поддържането и развитието на университетската информационна и комуникационна инфраструктура.

(4) Основните задачи на сектор „Информационни технологии и комуникации“ са следните:

1. да поддържа и развива потребителски ориентирана опорна университетска компютърна мрежа (УКМ), следваща организационната структура на УХТ, със запазване на автономността на отделните основни звена и отдели;
2. да проектира, развива и усъвършенства университетските информационни системи на базата на интегрираната компютърна инфраструктура;
3. да администрира система от информационни сървъри за управление на общи университетски дейности в сферите образование (например дистанционно обучение), наука, управление, финансово-счетоводство и др.;
4. да предлага на потребителите информационни услуги по производство и разпространяване на печатни и мултимедийни материали, специализирани за обучение.

## **РАЗДЕЛ II**

### **Университетска компютърна мрежа**

**Чл. 3.** (1) Локалната компютърна мрежа представлява мрежа от тип “Ethernet” (10/100/1000 BASE-T) на определен брой персонални компютри от всички звена на УХТ.

(2) Мрежата е изградена на принципа „Мрежа с равноправен достъп” (Peer to Peer) и функционира под мрежовите протоколи на “Microsoft Windows”. Връзката с интернет се осъществява по оптична линия.

(3) За надеждна и безпроблемна интернет връзка на всеки един от компютрите, свързани в мрежата, е създаден и конфигуриран интернет комуникационен сървър.

(4) Комуникационният сървър дава възможност на всеки от свързаните в локалната мрежа компютри да се осъществява пълен комплект интернет услуги. Създадени са условия за непрекъснат – 24 – часов, достъп до пълния комплект интернет услуги.

**Чл. 4.** (1) Университетската компютърна мрежа се състои от опорна мрежа и локални мрежи, свързани в комуникационна инфраструктура.

(2) Общото управление на университетската компютърна мрежа се извършва от сектор „Информационни технологии и комуникации“ и включва планиране, организиране, осъществяване, документиране, мониторинг, профилактика и усъвършенстване на дейности и регламенти, отнасящи се до единната компютърна инфраструктура.

(3) Администрирането на опорната мрежа е основна задача на сектор „Информационни технологии и комуникации“ и включва:

1. експлоатация и техническо поддържане на опорни мрежови устройства и комуникационни средства на университетската компютърна мрежа;
2. отчитане на дейностите по поддържане на технологии и топологии на университетската компютърна мрежа, които предоставят възможности за интегриране на информационни и комуникационни ресурси на УХТ и отделни негови звена;
3. техническо поддържане и обслужване на сървъри за съхраняване и обработка на данни, предоставяне на услуги и др.;

4. осигуряване на връзката на университетската компютърна мрежа с национални и международни мрежи, центрове за данни и доставчици на разнотипни електронни услуги, в това число и интернет.

(4) Локални мрежи могат да бъдат обособени както за отделни университетски звена, така и за проектни екипи.

(5) Администраторите на информационни системи към „Център за проектна и информационна дейност” поддържат основните университетски сървъри: именен сървър (DNS), прокси-сървър (Proxy Server), пощенски сървър и сървър за интернет страници (Host Server) и отговарят за тяхната безпроблемна и непрекъсната работа.

### **РАЗДЕЛ III**

#### **Информационни системи**

**Чл. 5.** В УХТ се развиват интегрирани информационни системи от тип „електронен университет“, наречени „Система за дистанционно обучение“ и „Система за управление на работните процеси“, които предоставят отдалечен достъп на оторизирани потребители за осъществяване на дейности на базата на интеграция на разнотипни информационни системи, данни и компютърни мрежи.

**Чл. 6.** Преподаватели, служители и студенти на УХТ получават, право на достъп до информационните системи след като получат собствено потребителско име – идентификатор, и определени права за достъп, които задължително се регистрират в съответен информационен архив в УХТ.

**Чл. 7.** Компютърните ресурси са предназначени за изпълнението на задачите и постигането на целите на УХТ. Тяхната употреба трябва да се

вмества в професионалните задължения на съответния потребител, както е предвидено в структурата на УХТ.

## РАЗДЕЛ IV

### Права и задължения на потребителите

**Чл. 8.** (1) Всеки потребител (преподавател, служител или студент) има право на достъп:

1. до академичната мрежа на УХТ и такъв следва да му бъде осигурен;
2. до съществуващите безжични точки за достъп в университетската мрежа.

(2) Всеки университетски потребител разполага с единно уникално потребителско име и парола (акаунт) за оторизация и достъп до информационните системи, като няма право да го предоставя на други лица (на електронен или друг носител, вкл. и на администратори), както и да ползва потребителско име, което не притежава.

(3) Всеки университетски потребител има служебен имейл адрес в зоната на домейна `uft-plovdiv.bg`, на който се получават всички служебни съобщения.

(4) Потребителите могат да използват предоставените им права само във връзка с извършвани от тях университетски дейности. Други дейности (вкл. получаване и изпращане на лична поща, съхраняване на лични материали и др. подобни) се разрешават само ако това не противоречи на някое от останалите правила и не е в разрез с политиката за сигурност за университетската компютърна мрежа и университетските информационни ресурси.

(5) Потребителите ползват университетската компютърна мрежа и университетските информационни ресурси само в рамките на предоставените им права за достъп и само чрез личния си акаунт. При неспазване на това

правило достъпът на нарушителя се ограничава или прекратява без предупреждение.

(6) Настройките при включване на сървър със стационарен IP адрес се одобряват от администратора на университетската компютърна мрежа, а при включване на нова работна станция – и от администратора на съответната локална мрежа.

## РАЗДЕЛ V

### Ограничения и забрани

**Чл. 9.** Забранява се на администраторите да съхраняват или инсталират нелицензиран софтуер в работни станции, мрежови сървъри на университетската компютърна мрежа.

**Чл. 10.** (1) На потребителите се забранява да създават, разполагат, рекламират, разпространяват и използват софтуер или данни (изображения, аудио-материали, текст и др.) в университетската компютърна мрежа и университетските информационни ресурси, които:

1. пропагандират антихуманни или расистки възгледи;
2. не са регистрирани (лицензирани) или нарушават авторско или патентно право;
3. имат за цел (преднамерено или не) да увредят целостта и сигурността на университетската компютърна мрежа и университетските информационни ресурси;
4. засягат правото за неприкосновеност на личната информация, като публикуват данни без изричното съгласие на засегнатото лице;
5. не са свързани с дейността на УХТ;

6. ограничават или правят невъзможен достъпа на други потребители до университетската компютърна мрежа и университетските информационни ресурси;

7. имат клеветнически, заплашителен или изнудващ характер.

(2) На потребителите се забранява да експлоатират университетската компютърна мрежа и университетските информационни ресурси в полза или във връзка с дейности (вкл. реклама, проучвания, услуги) на частни фирми, други физически или юридически лица, както и за собствена финансова или друга изгода без изрична заповед на Ректора.

(3) На потребителите се забраняват действия (вкл. ползване на университетските компютърни зали и компютърни лаборатории за свободен достъп), насочени към заобикаляне или премахване на защитни механизми на УХТ, университетската компютърна мрежа и университетските информационни ресурси, към затрудняване на работата на университетската компютърна мрежа, към ограничаване на достъпа и/или на правата на други потребители или за неправомерна промяна или разрушаване на целостта на данните в университетските информационни ресурси.

(4) На потребителите се забранява да съхраняват или инсталират нелицензиран софтуер в определените им потребителски директории на работни станции или мрежови сървъри на университетската компютърна мрежа, до които имат достъп.

(5) Забранява се копиране и използване на софтуер и данни, принадлежащи на друг потребител, без неговото изрично разрешение.

(6) Забранява се потребителите да използват университетската компютърна мрежа за разполагане и организиране на компютърни игри, освен ако това не е свързано с дейността на УХТ.

(7) На потребителите се забранява:



1. да правят опити за проникване в чужди мрежи и системи, до които нямат легитимен достъп;
2. да използват чужди изчислителни и комуникационни ресурси без изричното съгласие на собственика им;
3. да променят MAC и/или IP адреса на включеното в мрежата компютърно оборудване, както и да ги фалшифицират (spoofing);
4. да прилагат атаки от тип "отказ от обслужване" (Denial of Service), в това число flood (от всякакъв тип), Smurf и др.;
5. да прилагат методи за непозволено пренасочване на мрежовия трафик, в това число ARP spoof, ICMP redirect, DNS Redirect, физ. въздействие и др.;
6. да прилагат методи за непозволено подслушване на мрежовия трафик (sniffing);
7. да разпространяват програми от тип "Троянски кон", червеи и вируси и друг злонамерен програмен код, включително и неумишлено;
8. да използват приложения, даващи нелегитимен достъп до чужди системи или водещи до отказ от обслужване в последните (exploits, DoS и т.н.), включително и неумишлено;
9. да свързват допълнително мрежово оборудване към мрежата на УХТ без знанието и разрешението на администраторите на мрежата;
10. да препродават или предоставят/преотстъпват достъпа си до мрежата на трети лица.

(8) Като умишлени действия се класифицират тези със следните характеристики:

1. ненужно изразходване на усилията на персонала или на мрежовите ресурси, включително и ненужно изразходване на процесорно време на крайни системи, и на усилията на персонала, поддържащ тези системи;
2. повреждане или унищожаване на данни на други потребители;

3. нарушаване на правото на лична тайна на други потребители;
4. продължаване на използването на мрежови програми или устройства, след като системните администратори на мрежата са поискали преустановяването му, тъй като те възпрепятстват нормалното функциониране на мрежата.

## РАЗДЕЛ VI

### Санкции

**Чл. 11.** (1) При възникване на проблеми при функционирането, експлоатацията или осигуряването на сигурността на университетската компютърна мрежа университетските информационни ресурси, администраторите към „Център за проектна и информационна дейност” могат да преустановят достъпа на конкретен потребител или група потребители (или да изключат връзките на устройство или група устройства) за 24 часа.

(2) Потребителското име (акаунт) може да се блокира без предупреждение. Нарушението може да попадне под действието и на други закони на Република България.

(3) Връзките на устройство или група устройства в университетската компютърна мрежа могат да бъдат изключени без предупреждение до отстраняване на нарушението/проблема.

**Чл. 12.** При необходимост, локалните администратори предприемат срочно мерки по прекъсване и ограничаване на потребителския достъп до възстановяване на нормалната работа на университетската компютърна мрежа.

**Чл. 13.** При неспазване от страна на потребителите на установените правила за ползване на университетската компютърна мрежа и

университетските информационни ресурси се налагат и наказания съгласно Кодекса на труда.

*Настоящият Правилник е приет с решение на Академичния съвет,  
Протокол № 19 /31.03.2017 г.*