Финансирано от Европейския съюз
NextGenerationEU

Тема 2.5. Онлайн етикет

МУЛТИМЕДИЕН ТЕКСТ (ПОМАГАЛО) ТИП ЛЕКЦИЯ (УЧЕБНИК)

Съдържание

1 Тук ще научите

- Какви са основните правила на поведение, правата и отговорностите за етично използване на дигитални устройства и средства в различни дигитални среди.
- Как да разпознавате и използвате добри и лоши практики при използване на дигиталните технологии и интернет.
- Какви са нормативната база и видовете дигитални престъпления (на базово ниво).

1.1 Ново понятие

Понятие	Описание
Онлайн етикет и правила на поведение в интернет	Норми на етично поведение и общуване между хората в Интернет пространството, познати и като „нетикет“.

2 Основни правила на поведение в интернет

Всяко едно общество или среда има своите гласни и негласни норми и правила за етично поведение. Що се отнася до интернет, тези норми и правила са познати под събирателното понятие *Нетикет*.

2.1 Нетикет

За да разберем по-добре този термин, нека видим по-внимателно неговата етимология (произход):

- Етикет – обноски, изисквани от доброто възпитание или наложени авторитетно като задължителни в социалния или официален живот
- Etiquette – от френски буквално означава „билет“, а „етикет“ в случая – входен билет за определена група или общество
- Нетикет – съкратено от *Интернет етикет* (Netiquette = Internet Etiquette) – норми на етично поведение и общуване между хората в интернет пространството.

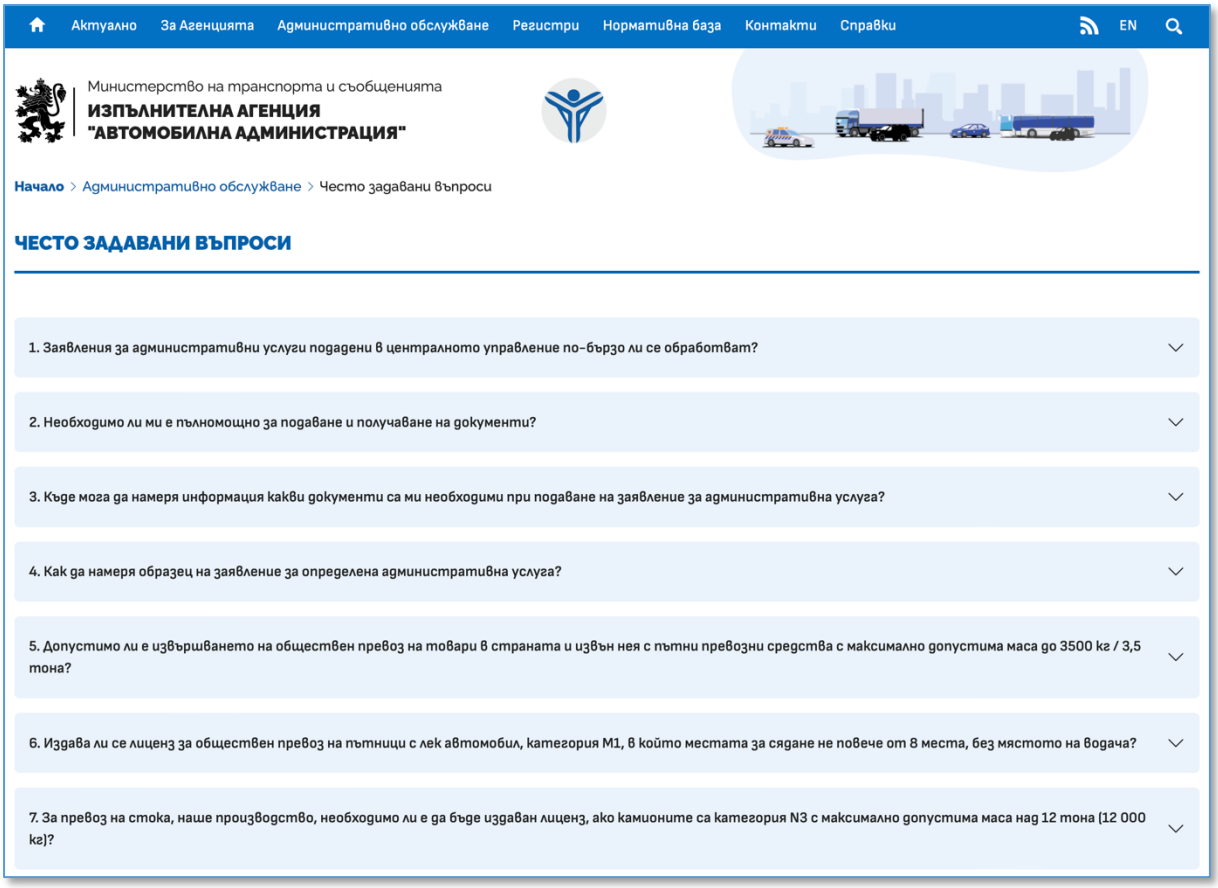
Основните правила на етично поведение засягат съдържанието и формата на общуване и зависят от вида на комуникацията, която може да е:

- междуличностна или групова
- формална (делова) или неформална
- частна или публична
- синхронна или асинхронна
- на роден или на чужд език.

В по-синтезиран вид, най-важните правила на *нетикета* са:

- Не забравяйте, че отсреща също стои човек
- Спазвайте правилата от реалния живот
- Помнете къде се намирате (форум, група в социална мрежа и др.)
- Ценете времето на другите, както цените своето
- Изглеждайте добре в мрежата (ако комуникирате с включена камера)
- Избягвайте конфликти
- Уважавайте личната неприкосновеност
- Не превишавайте и не злоупотребявайте с правата си
- Всеки прави грешки

Правилата за поведение са общоприети, макар че различните общности могат да въвеждат свои допълнителни специфични изисквания. По тази причина се препоръчва, когато потребителят попадне в нова общност, първо да прочете нейните „Често задавани въпроси“ (FAQ – *frequently asked questions*, Фиг. 1) и да прекара известно време като наблюдател, преди сам да започне да взема участие в комуникационния процес.



Фигура 1: Пример за секция с често задавани въпроси.

Правилата на нетикета засягат както съдържанието, така и формата на общуване.

По отношение на съдържанието недопустими според нетикета са отправянето на обиди и заплахи, намесите в личните пространства, рекламирането извън създадените за тази цел бизнес мрежи. В различните общности има и различна степен на толерантност към дискусиите извън темата (т.нар. *Off-topic discussions*).

По отношение на формата, според нетикета на много общности писането изцяло с главни букви е израз на агресия.

Нетикетът съобразява общуването и с ограниченията на средата – текстуалния канал, при който по-трудно се предават интонацията и емоциите, които достигат до събеседниците при едно живо общуване. Затова нетикетът насърчава потребителите да използват емотикони, винаги когато това е уместно или наложително.

При всичките различия между нетикета на различните общности, едно правило е общовалидно и обикновено поставяно на първо място в ръководствата: „Никога не забравяйте, че отсреща стои човек, когото можете да нараните емоционално.“ Или както го формулира авторката на първата книга по нетикет, Виржиния Ший: „В интернет никога не бива да правиш нещо, за което смелостта не би ти стигнала на живо“.

2.2 Правила и отговорности за етично използване на дигитални устройства в различни дигитални среди

2.2.1 Анонимни ли сме в интернет?

Задавали ли сте си въпроса доколко сте анонимни в интернет пространството? Дори когато не използваме истинското си име, а например псевдоним, нашата самоличност може да бъде разкрита чрез електронния адрес в интернет мрежата, която ползваме (т.нар. *IP адрес* – Internet Protocol адрес), както и чрез уникалния идентификационен номер на устройството, което ползваме (т.нар. *MAC адрес* – Media Access Control адрес). Именно затова следва да сме още по-отговорни и да се стремим да спазваме правилата за етично поведение. Повече по темата за видимостта на самоличността в интернет ще научите в следващата тема, а именно в темата за управление на дигиталната идентичност.

2.2.2 Правила, свързани с електронна поща

При комуникацията по електронна поща има важни общовъзприети норми и правила, които е добре да имате предвид.

Критични за първоначално впечатление са обръщението, оформлението, стила на писане, езика, правописа, пунктуацията.

Електронният адрес е важен – дали пишете от личен такъв или от служебен. При формално общуване не е в нормата да ползвате личен имейл адрес.

Темата на съобщението следва да е добре формулирана, да е кратка (до няколко думи) и ясна. Липса тема или тема, звучаща като реклама, е предпоставка

писмото ви автоматично да бъде възприето като нежелана поща (*bulk, spam, junkmail*) и да бъде блокирано или поставено в папка *Спам*.

Следвайте принципа „едно писмо една тема“, т.е. ако искате да засегнете няколко различни теми и въпроси, свързани с тях, отделете ги в отделни писма, като ги означите с различно озаглавени теми в полето за задаване на тема.

При отговор или препращане на писмо, обърнете внимание, че автоматично се появяват съответно *Re:* или *Fwd:* в началото на темата. Не ги изтривайте! Това са важни индикатори, че писмото ви е отговор на друго или че препращате чуждо писмо.

Ако пишете за първи път на някого, не забравяйте да се представите с няколко думи в началото, а в края на писмото напишете името и координатите си.

Ако изпращате прикачени файлове към писмото си, уточнете това в текста – какво точно изпращате като съдържание.

Ако писмото ви е делово, имайте предвид, че не е прието да използвате емотикони. Нека те останат за по-личната комуникация. ☺

2.2.3 Верижни писма

Верижното писмо (от англ. ез. – *chain letter*) е съобщение, което се опитва да убеди получателя да направи няколко копия на писмото и да ги изпрати на определен брой получатели. Получава се разрастваща се „верига“ – нещо като пирамида.

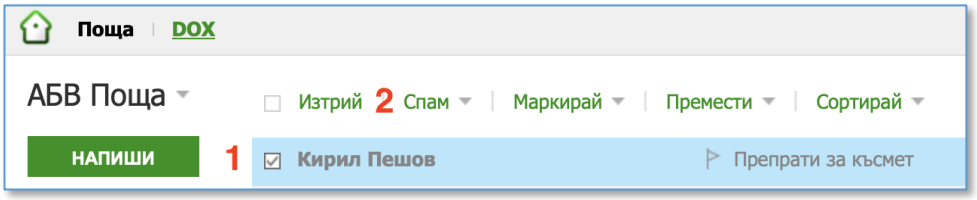
Обичайните методи, използвани във верижните писма, включват емоционално манипулативни истории, пирамидални схеми за бързо забогатяване и използване на суеверия за заплашване на получателя. Първоначално верижните писма са били хартиени писма, изпращани по стандартната поща. Днес верижните писма често се изпращат по електронен път чрез електронна поща, сайтове на социални мрежи и текстови съобщения.

Някои имейл съобщения, изпратени като верижни писма, могат да изглеждат съвсем безобидни. Например ученик от гимназията, който иска да провери колко души могат да получат неговия имейл за научен проект.

Съобщенията понякога включват фалшиви обещания от компании или богати хора (като Бил Гейтс), които обещават парична награда на всеки, който получи съобщението. Те могат да бъдат и политически мотивирани или предупреждение, че популярно телевизионно или радиопредаване може да бъде свалено от ефир. Някои, като хавайския тотем за късмет, който се разпространява в хиляди форми, заплашват потребителите с лош късмет, ако не го препратят. Съществуват много форми на верижни имейли, които заплашват със смърт или отнемане на душата, като разказват истории за смъртта на други хора.

Друга разпространена форма на верижно писмо по електронна поща е измамата с вирус и форма на кибертормоз.

Важно е да запомним, че не бива да препращаме подобни писма и съобщения! Най-разумно е да ги преместим в папка *Спам*, по възможност без да ги отваряме: маркирайте писмото, поставяйки отметка в полето в началото на ред, и щракнете върху надписа *Спам* (Фиг. 2).



Фигура 2: Примерно верижно писмо.

3 Добри и лоши практики при използване на дигиталните технологии и интернет

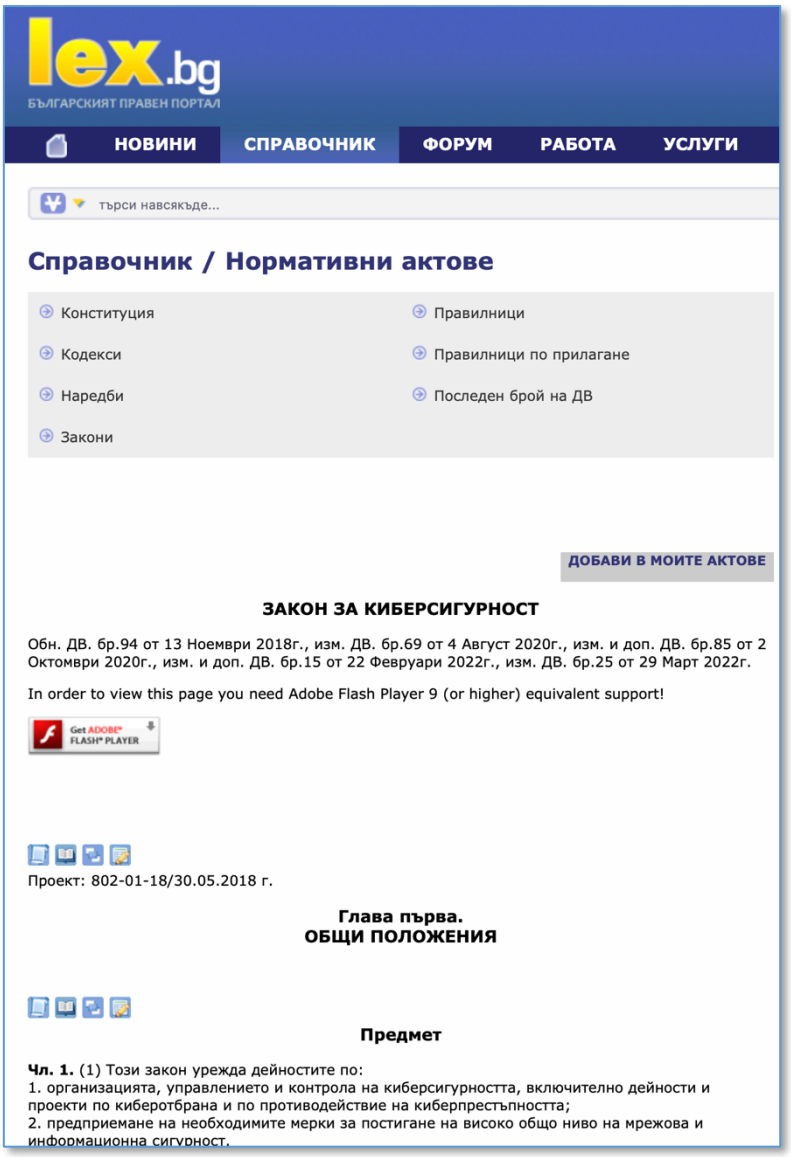
Интернет днес е напълно естествена част от живота ни и много от нас не могат да си представят как нашите баби и дядовци например са се справяли без електронна поща, игри, видеоклипове или търсене на отговор на въпрос в мрежата. Да не говорим колко приятно е да си чатиш с приятелите си и когато ти се случи нещо интересно, да им съобщиш за това и дори да им изпратиш снимка.

В някои случаи дори можем да кажем, че интернет вече е почти истински живот за нас. Обаче, както видяхме вече, подобно на реалния живот, има определени правила, които трябва да спазваме по отношение на поведението си в интернет. Само защото сте на компютъра и привидно никой не може да разбере кой сте и какви са намеренията ви, общата учтивост диктува, че трябва да се държите по определен начин, т.е. да спазвате нетикета или с други думи – да имаме добри маниери онлайн. Точно както има определени правила, които спазваме, когато сме в училище или в магазина, има и други правила, които трябва да спазваме онлайн, така че времето ни в интернет да остане приятно.

Добрите практики при използване на дигиталните технологии и интернет са именно случаите, когато се спазват нормите и правилата на поведение, описани в темата до тук. Всички останали случаи се определят като лоши практики и тяхната най-крайна форма са дигиталните престъпления, по-познати с термина *киберпрестъпления*.

3.1 Нормативна база

Нормативната база в Република България, свързана с киберпрестъпността, е описана подробно в Закона за киберсигурност (Фиг. 3), който може да бъде достъпен и разгледан на следния интернет адрес:
https://lex.bg/bg/laws/ldoc/2137188253



Фигура 3: Закон за киберсигурност, достъпен в сайта lex.bg.

3.2 Видове дигитални престъпления

Киберпрестъпленията обхващат широк спектър от дейности. В единия край са престъпленията, които включват фундаментални нарушения на личната или корпоративната неприкосновеност на личния живот, като посегателства срещу целостта на информацията, съхранявана в цифрови хранилища, и използването на незаконно получена цифрова информация за тормоз, увреждане или изнудване на фирма или лице, както и нарастващото престъпление, известно като *кражба на самоличност*.

В средата на този спектър се намират престъпления, основани на транзакции, като измама, трафик на детска порнография, цифрово пиратство, пране на пари и фалшифициране. Това са специфични престъпления с конкретни жертви, но престъпникът се крие в относителната анонимност, която предоставя интернет. Друга част от този вид престъпления включва лица в корпорации или държавни

бюрокрации, които умишлено променят данни с цел печалба или политически цели. В другия край на спектъра са престъпленията, които включват опити за нарушаване на действителното функциониране на интернет. Те варират от спам, хакерски атаки и атаки за отказ на услуга срещу конкретни сайтове до актове на кибертероризъм, т.е. използване на интернет за предизвикване на обществени безредици и дори смърт. Кибертероризмът се фокусира върху използването на интернет от недържавни субекти за въздействие върху икономическата и технологичната инфраструктура на дадена страна. След атентатите в САЩ, случило се на 11 септември 2001 г., обществената осведоменост за заплахата от кибертероризъм нарасна значително.