VI.
BEZPIECZEŃSTWO W KOMUNIKACJI I MEDIACH

Edukacja formalna – dzieci

Zagadnienia	Wychowanie przedszkolne	Szkoła podstawowa, klasy 1-3	Szkoła podstawowa, klasy 4-6
Ochrona prywatności i wizerunku	• umie zakomunikować, że się wstydzi i nie chce uczestniczyć w danej sytuacji komunikacyjnej; np. nie chce być nagrywane lub fotografowane, nie chce rozmawiać przez telefon.	• wie, że pewnych informacji nie wolno udostępniać obcym; w razie wątpliwości pyta rodziców lub opiekunów. • umie odróżnić uwiecznienie od upublicznienia. • umie sprzeciwić się innemu dziecku lub dorosłemu w kwestii publikacji swojego utworu lub związanej z wizerunkiem; np. pokazywanie filmu z jego udziałem.	• umie wskazać różnice pomiędzy komunikacją prywatną i publiczną.
Anonimowość		• wie, co to znaczy „anonimowość”.	• wie, że z sieci możemy korzystać anonimowo. • umie podać przykład sytuacji, w której anonimowość jest wskazana.
Bezpieczeństwo komunikacji, pracy i transakcji	• umie zakomunikować, że dana treść budzi strach lub poczucie zagrożenia, ale niekoniecznie umie temu zaradzić, np. celowo przełączyć kanał.	• rozumie, co to „sekret”, „tajemnica” i umie jej dochować, również w sytuacji komunikacyjnej. • umie selekcjonować treści, które odbiera; np. poprzez wyłączenie telewizora, zmianę filmu, zmianę strony.	• wie, że pewne informacje i rodzaje komunikacji powinny być „tajemnicą” (np. hasło do poczty). • wie, że istnieją sposoby zapewnienia tej „tajemnicy” i umie o nie spytać. • wie, że zakupy można zrobić w fizycznym sklepie, jak i w sklepie internetowym czy portalu aukcyjnym; potrafi podać przykłady. • wie, co to spam i umie rozpoznać bardziej oczywiste jego przykłady.
Nadzór nad siecią			• wie, co to znaczy „cenzura”. • wie, co to znaczy „podsłuchiwać”, również w kontekście technologii i sieci; np. wie, że kiedy pisze do kogoś w internecie, czyta to też jeszcze ktoś inny.
Uzależnienia i higiena korzystania z mediów			• umie dostrzec sytuacje, w których przekroczone zostają granice higieny korzystania z mediów; np. mama za dużo gra w gry, kolega za dużo rozmawia przez telefon. • wie, że relacje przez media mają wpływ na relacje bezpośrednie, a czynności dokonywane przez media mogą mieć bardzo realne konsekwencje (np. płatności).

Edukacja formalna – młodzież

Zagadnienia	Gimnazjum	Szkoła ponadgimnazjalna	Szkolnictwo wyższe
Ochrona prywatności i wizerunku	• umie zdecydować, czy w danej sytuacji komunikacja powinna być prywatna czy publiczna.	• umie poprawnie zidentyfikować, czy dane narzędzia (np. czat na portalach społecznościowych) faktycznie oferują komunikację prywatną, czy tylko jej złudzenie. • umie posłużyć się narzędziami zwiększającymi prywatność; np. rozszerzenia przeglądarek, ustawienia prywatności. • wie, do czego służą regulaminy na stronach, z których korzysta.	• umie płynnie posługiwać się metodami i narzędziami ochrony prywatności. • czyta ze zrozumieniem regulaminy stron, z których korzysta, i umie świadomie podjąć decyzje dotyczące przyjęcia lub odrzucenia ich postanowień.
Anonimowość	• wie, że są specjalne narzędzia do zwiększania anonimowości w sieci i umie o nie spytać. • wie, że anonimowość w sieci może być pozorna i że często możliwe jest ustalenie autora danej informacji nawet jeżeli używał pseudonimu. • wie, że jeżeli ujawni w treści komunikacji dane identyfikujące, sam fakt komunikowania się anonimowo (np. przy użyciu odpowiednich narzędzi) nie wystarczy do zachowania anonimowości.	• umie posłużyć się narzędziami zwiększającymi anonimowość; np. TOR, anonimowe proxy, dystrybucja Linuksa TAILS.	• świadomie i trafnie podejmuje decyzje dotyczące anonimowości w różnych sytuacjach komunikacyjnych; np. świadomie w pewnych sytuacjach wyłącza usługi lokalizacyjne dostępne w przeglądarce.
Bezpieczeństwo komunikacji, pracy i transakcji	• wie, że dane prywatne mogą być traktowane jak towar. • umie skorzystać z podstawowych narzędzi zapewniających bezpieczeństwo komunikacji; np. korzysta z https na stronach banków czy portalach społecznościowych. • wie, że należy wylogować się z portali po zakończeniu pracy. • wie, że są różne formy płatności w internecie o różnym poziomie bezpieczeństwa. • zna podstawowe zasady bezpieczeństwa przy zakupach on-line.	• z dużą dozą pewności rozpoznaje spam i próby phishingu; np. zwraca uwagę na to, że nie zgadza się adres strony bankowej. • zwraca uwagę na certyfikaty; np. nie akceptuje automatycznie każdego napotkanego błędnego certyfikatu zgłoszonego przez przeglądarkę. • wie, że istnieją narzędzia dodatkowo zwiększające bezpieczeństwo komunikacji i umie do nich dotrzeć; np. szyfrowanie end-to-end, poczty, PGP/GPG, OTR.	• płynnie posługuje się narzędziami zwiększającymi bezpieczeństwo komunikacji. • zna narzędzia szyfrowania end-to-end i umie ich użyć np. PGP/GPG, OTR.

Zagadnienia	Gimnazjum	Szkoła ponadgimnazjalna	Szkolnictwo wyższe
Nadzór nad siecią	• wie, że sieć może być nadzorowana. • wie, że nadzór ten może mieć wiele form, w tym cenzury czy podsłuchu. • wie, że nadzór może nie być zauważalny dla nadzorowanych; np. zdaje sobie sprawę, że skutkiem nadzoru może być trudna do identyfikacji zmiana wyników wyszukiwania.	• wie, że mogą być różne cele wprowadzania nadzoru i umie je wymienić; np. ochrona dzieci w internecie; uzyskiwanie dodatkowych przychodów przez daną korporację ze sprzedaży prywatnych danych użytkowników. • wie, że nadzór może być legalny lub bezprawny; że może być prowadzony przez organa państwowe (np. policję) i osoby prywatne czy korporacje. • wie, że istnieją metody obejścia/utrudnienia nadzoru, nie tylko techniczne; np. potrafi wymienić takie metody jak świadome umieszczanie informacji fałszywych lub stosowanie szyfrowania nie tylko do treści wrażliwych, ale również banalnych, celem utrudnienia identyfikacji, kiedy zachodzi ważna/wrażliwa komunikacja.	• umie korzystać z narzędzi obejścia/utrudnienia nadzoru. • świadomie podejmuje decyzje o doborze narzędzi do konkretnych celów, biorąc pod uwagę możliwość nadzoru osób trzecich nad tymi narzędziami, oraz specyfikę treści.
Uzależnienia i higiena korzystania z mediów	• wie, że pewne wzorce zachowań mogą prowadzić do uzależnienia. • umie zidentyfikować niebezpieczne wzorce i ich unikać. • wie, czym jest stalking (nękanie).	• umie świadomie kształtować swoje nawyki związane z korzystaniem z technologii. • umie zaobserwować oznaki uzależnienia u siebie i u innych. • umie przewidzieć konsekwencje działań w sieci, które mogą spowodować groźne sytuacje także poza nią; np. nie podaje publicznie informacji o planowanej dłuższej nieobecności w domu na portalu społecznościowym, na którym podany jest również adres zamieszkania. • umie rozpoznać stalking (nękanie) i wie, jak się przed nim bronić. • umie zarządzać wizerunkiem on-line; świadomie podejmuje decyzję, na ile wizerunek on-line odzwierciedla jego prawdziwą tożsamość; np. nie publikuje danych umożliwiających odkrycie jego tożsamości.	• umie zareagować na negatywne wzorce zachowań u innych, np. szukając pomocy specjalisty. • dostrzega powiązania pomiędzy swoimi działaniami w mediach a innymi sferami życia, umie tymi powiązaniami zarządzać.

Kształcenie ustawiczne

Zagadnienia	Poziom minimum	Poziom optimum	Poziom mistrzowski
Ochrona prywatności i wizerunku	• wie, że prywatność jest dobrem i że mamy do niej prawo. • wie, że ochrona wizerunku wymaga ochrony prywatności. • wie, że dane prywatne mogą być traktowane jak towar. • wie, że pewne komunikaty mogą być przekazywane wyłącznie prywatnie, a inne udostępniane publicznie. • rozumie, że biorąc udział w komunikacji, potencjalnie odpowiada za wizerunek nie tylko swój, ale np. swojego pracodawcy, jeśli używa np. firmowego adresu e-mail.	• umie używać podstawowych narzędzi chroniących prywatność, np. rozszerzenia do przeglądarek, blokada ciasteczek. • umie precyzyjnie wskazać, które, komunikaty mogą być przekazywane wyłącznie prywatnie, a które udostępniane publicznie. • wie, że nawet dane anonimizowane zebrane w odpowiedniej ilości mogą pozwolić na naruszenie prywatności. • wie, że jego decyzje dotyczące prywatności mogą różnić się od decyzji innych i umie to uszanować. • umie dostosować swój wizerunek do sytuacji i roli.	• świadomie kreuje swój wizerunek on-line w różnych kontekstach. • płynnie posługuje się technikami i narzędziami ochrony prywatności. • umie świadomie podejmować decyzje dotyczące udostępnienia bądź nie danych swoich i swoich znajomych, uwzględniając ich preferencje w zakresie ochrony prywatności i wizerunku.
Anonimowość	• wie, że z sieci możemy korzystać anonimowo. • wie, że korzystanie anonimowe nie wyklucza możliwości ustalenia autora. • wie, że istnieją metody śledzenia osób w sieci bez ich wiedzy, np. ciasteczka.	• wie, że istnieją narzędzia zwiększające anonimowość (jak rozszerzenia do przeglądarek, systemy TOR, I2P, proxy). • umie znaleźć i dostosować do swoich potrzeb ustawienia przeglądarek zwiększające anonimowość.	• biegle korzysta z narzędzi i technik zapewniających anonimowość w sieci. • umie kompleksowo zadbać o zachowanie anonimowości, korzystając z kombinacji narzędzi, np. tryb prywatny, TOR, blokada ciasteczek.

Zagadnienia	Poziom minimum	Poziom optimum	Poziom mistrzowski
Bezpieczeństwo komunikacji, pracy i transakcji	• umie skorzystać z podstawowych narzędzi zapewniających bezpieczeństwo transmisji (https). • wie, że należy wylogować się po zakończeniu pracy na publicznym terminalu lub w sytuacji, w której inni będą korzystać z tego samego komputera. • zwraca uwagę na ostrzeżenia o wygasłych/nieprawidłowych certyfikatach, w razie wątpliwości pyta (nie akceptuje automatycznie). • docenia wagę traktowania pewnych informacji jako tajnych, zdaje sobie sprawę, że dzielenie się hasłami (nawet jeśli np. zwiększa wygodę) jest niedopuszczalne. • potrafi zachować „higienę informatyczną”, np. zwraca uwagę na komunikaty pojawiające się na ekranie i nie akceptuje rzeczy, których nie rozumie – w takich sytuacjach pyta; zdaje sobie sprawę z zagrożeń takich jak wirusy; potrafi korzystać z tzw. „trybu prywatnego” przeglądarek.	• umie samodzielnie podjąć decyzję dotyczącą bezpieczeństwa komunikacji w danym przypadku, np. decyduje o zaakceptowaniu bądź nie wygasłego/nieprawidłowego certyfikatu. • zdaje sobie sprawę z zagrożeń związanych ze scentralizowanymi sieciami i usługami; umie podać przykłady sieci scentralizowanych (np. Facebook, Google) oraz zagrożeń z nimi związanych (np. utrata kontroli nad komunikacją, podsłuch).	• płynnie posługuje się systemami szyfrowania end-to-end (PGP/GPG, OTR). • śledzi najważniejsze doniesienia dotyczące naruszeń bezpieczeństwa i umie wdrożyć rozwiązania problemów oraz sugerowane praktyki. • podejmuje świadome, oparte na rzetelnych przesłankach decyzje dotyczące narzędzi, których używa, biorąc pod uwagę również przesłanki pozatechniczne; np. bierze pod uwagę to, czy wszystkie kanały komunikacji, z których korzysta, mogą być łatwo kontrolowane przez jedną organizację. • rozumie zalety decentralizacji i umie je uwzględnić w podejmowanych decyzjach. • potrafi przeprowadzić prosty, nieformalny audyt bezpieczeństwa, wskazując na braki w danej sytuacji; np. doradza szyfrowanie.
Nadzór nad siecią	• wie, że komunikacja w sieci może być nadzorowana w sposób niezauważalny dla korzystającego. • wie, że istnieją narzędzia obchodzące nadzór, umie znaleźć informacje na ich temat. • wie, że nadzór może być legalny lub bezprawny; prywatny i państwowy. • wie, że nadzór może prowadzić do cenzury.	• umie skorzystać samodzielnie z podstawowych narzędzi walki z potencjalnym nadzorem w sieci. • wie, że nadzór nad komunikacją w sieci jest wielopoziomowy. • umie rozpoznać, które kanały komunikacji są bardziej podatne na nadzór od innych. • umie podać przykłady sytuacji, w których nadzór jest uzasadniony, i takich, w których nie jest.	• umie aktywnie przeciwdziałać nadzorowi w sieci, świadomie stosując wiele technik w tym celu. • umie z dużą dozą pewności określić, które kanały komunikacji są najprawdopodobniej nadzorowane i w jakich celach.
Uzależnienia i higiena korzystania z mediów	• wie, że pewne wzorce zachowań mogą prowadzić do uzależnienia. • wie, że relacje przez media mają wpływ na relacje bezpośrednie a czynności dokonywane przez media mają bardzo realne konsekwencje (np. płatności). • umie przewidzieć konsekwencje działań w sieci, które mogą spowodować groźne sytuacje także poza nią. • wie, czym jest stalking i umie go rozpoznać.	• umie zidentyfikować niebezpieczne wzorce zachowań i unikać sytuacji, które do nich prowadzą. • umie świadomie kształtować swoje nawyki związane z korzystaniem z technologii. • umie zaobserwować oznaki uzależnienia u siebie i u innych. • zna podstawowe narzędzia i metody obrony przed zagrożeniami związanymi z komunikacją przez media.	• umie zareagować na negatywne wzorce zachowań, np. szukając pomocy specjalisty. • umie zidentyfikować próby aktywnych ataków w środowisku medialnym (phishing targetowany) i się przed nimi obronić.