NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

PROFIL ŽÁKA STŘEDNÍ ŠKOLY

www.nukib.cz

PROFIL ŽÁKA STŘEDNÍ ŠKOLY

Vycházíme z toho, že žáci umí vše, co měli umět ze základní školy. Současně je materiál určen pouze pro výuku všeobecného základu. Předměty, zaměřené na komunikační techniku v rámci odbornosti je nutné uzpůsobit konkrétnímu zaměření a specializaci oboru.

Základním požadavkem je to, aby ze střední školy neodešel nikdo, kdo nebude mít alespoň základní znalosti – tedy **ve všech oblastech bude na úrovni I**. Vždy tedy začínáme testováním a poté se musíme věnovat doladění rozdílných znalostí žáků na výchozí úroveň.

Dále se pak dá odpíchnout od počtu hodin a zaměření oboru – je na každém učiteli, aby se rozhodl, co je pro jeho žáky podstatné. Je jasné, že žáci učebního oboru Elektromechanik - sdělovací a zabezpečovací technika budou mít výrazně jiné znalosti než žáci oboru Pečovatel nebo Pekař a to i přesto, že mají podobný počet hodin.

Je nutné také zdůraznit, **že řada oborů**, ať už učebních, nebo maturitních, **má další předměty, ve kterých se bezpečnost probírá automaticky**. Jedná se nejen o obory technické, ale i o práci v administrativě nebo obory medicínské.

Stejně tak absolventi gymnázií nebudou mít těžiště bezpečnosti v technickém zabezpečení sítí, ale budou mít určitě široký rozhled, pokud jde o bezpečnost na úrovni soft skills.

V následujícím textu se pokusíme jednotlivé kategorie žáků shrnout.

Postup učiva bude vycházet z klasického rozložení současnosti: hardware, software, komunikační dovednosti. Tato tradice je nicméně dost stará a v současné době se uplatňuje přístup opačný, tedy nejprve se naučit danou věc používat, pak na základě správného použití porozumět její funkci a nakonec i technickým finesám. Necháme na každém učiteli, jestli půjde cestou tradice nebo nových metod. Materiál to umožňuje, celky v něm jsou uzavřené.

PROFIL PRO DOTACI 3 X 1 HODINY:

Profil je určen pro žáky převážně tříletých oborů. Většinou mají praktické sklony a touhu experimentovat, je tedy vhodné posílit technickou část a naučit žáky i správnou terminologii, pokud jde o další znalosti. Rizikem bývá často podceňování těchto žáků, kteří mohou být digitálně velmi zdatní, občas bohužel zdatnější, než pedagogové.

DOPORUČENÝ PRŮCHOD U TECHNICKÝCH OBORŮ A ZVÍDAVÝCH TŘÍD:

Základní technické znalosti II.

Základní znalosti v oblasti software, zejména aplikací II.

Základní znalosti v oblasti komunikace I.

DOPORUČENÝ PRŮCHOD U NETECHNICKÝCH OBORŮ:

Základní technické znalosti I.

Základní znalosti v oblasti software, zejména aplikací I.

Základní znalosti v oblasti komunikace II.

PROFIL PRO DOTACI 2 X 2 HODINY

Profil je určen pro dotaci 4 hodiny, kdy obvyklé rozložení je 2 x 2 hodiny. Předpokladem je, že žáci nemají pouze obecné ICT, ale navazují nějakými dalšími, specializovanými předměty, do jejichž výuky budou zahrnuta specifika, daná jejich zaměřením. Například absolvent oboru „Veřejnosprávní činnost“ bude vyžadovat znalosti z oběhu dokumentů, evidenci a práci se spisovou službou, která se učí ve specializovaných předmětech a bezpečnost, týkající se těchto činností, bude zahrnuta tam. Podobnou dotaci mívají i gymnázia.

Z tohoto důvodu je zde posílena komunikační část a omezena část technická. Průchod už bude pouze jeden, dělení na technické a netechnické obory nemá význam, protože každý obor má svá specifika.

DOPORUČENÝ PRŮCHOD:

Základní technické znalosti I.

Základní znalosti v oblasti software, zejména aplikací II.

Základní znalosti v oblasti komunikace III.

PROFIL S DOTACÍ 8 HODIN

Je určen pro nejvyšší hodinovou dotaci na středních školách. Absolvent by měl být schopen samostatné správy stanic a zvládnout běžné bezpečnostní incidenty, stále je ale nutné mít na paměti, že jde o žáka střední školy a nelze po něm chtít totéž, jako po vysokoškolákovi nebo správci sítě s praxí. Ani v tomto případě není možné požadovat správu serverů nebo pokročilou správu sítě, pokud nejde o IT zaměření s další, rozšiřující výukou. Takové znalosti ale nejsou podchyceny v tomto dokumentu.

DOPORUČENÝ PRŮCHOD:

Základní technické znalosti III.

Základní znalosti v oblasti software, zejména aplikací III.

Základní znalosti v oblasti komunikace II.

OBSAHY JEDNOTLIVÝCH ÚROVNÍ

ZÁKLADNÍ TECHNICKÉ ZNALOSTI

ZÁKLADNÍ TECHNICKÉ ZNALOSTI I.

- Žák dokáže určit parametry digitálního zařízení, potřebné pro daný typ činnosti, pokud má tento typ specifikován. Na základě toho je schopen určit základní bezpečnostní parametry.
- Detekuje závadové projevy technických zařízení, umí je správně popsat a ohlásit
- Chápe nutnost nastavení a aktualizací OS, firewallu a antiviru a při manipulaci s nimi dodržuje zásady bezpečnosti. Je schopen sám upravit základní nastavení firewallu.
- Umí rozpoznat zabezpečenou WiFi síť, připojit ji i odpojit

ZÁKLADNÍ TECHNICKÉ ZNALOSTI II.

- Žák dokáže určit parametry digitálního zařízení, potřebné pro daný typ činnosti, pokud má tento typ specifikován. Na základě toho je schopen určit základní bezpečnostní parametry.
- Dokáže nastavit bezpečnostní omezení a software na základní úrovni
- Detekuje závadové projevy a zvládne jednodušší opravy dle pokynů
- Chápe nutnost nastavení a aktualizací OS, firewallu a antiviru a při manipulaci s nimi dodržuje zásady bezpečnosti. Je schopen sám upravit základní nastavení firewallu. Umí provést běžný antivirový test a otestovat konkrétní adresář a soubor
- Umí rozpoznat zabezpečenou WiFi síť, připojit ji i odpojit
- Zná základní porty a protokoly a chápe nutnost jejich zabezpečení, používá VPN přístup

ZÁKLADNÍ TECHNICKÉ ZNALOSTI III.

- Žák dokáže určit parametry digitálního zařízení, potřebné pro daný typ činnosti. Na základě toho je schopen určit základní bezpečnostní parametry.
- Zná porty a protokoly, ví, které služby patří k rizikovým, chápe způsoby ochrany
- Chápe nutnost nastavení a aktualizací OS, firewallu a antiviru a při manipulaci s nimi dodržuje zásady bezpečnosti. Je schopen sám upravit základní nastavení firewallu. Umí provést běžný antivirový test a otestovat konkrétní adresář a soubor
- Ovládá základní pojmy z teorie sítí a základy nastavení sítě. Zná topologie a rizika sítí klient-server a typu P-2-P, zná běžné síťové prvky a termíny typu NAT, router a další
- Umí rozpoznat zabezpečenou WiFi síť, připojit ji i odpojit
- Zná rozdíly mezi protokoly zabezpečení WiFi, datovým připojením a VPN přístupem
- Zná základní porty a protokoly a chápe nutnost jejich zabezpečení, používá VPN přístup
- Je schopen správně provést základní postupy podle krizového plánu organizace, rozumí přijatým zásadám a dokáže je správně aplikovat na stanice v případě ohrožení

ZÁKLADNÍ ZNALOSTI V OBLASTI SOFTWARE

ZÁKLADNÍ ZNALOSTI V OBLASTI SOFTWARE I.

- Žák zná zásady bezpečného používání digitálních technologií včetně tvorby silného hesla
- Zná zásady práce se soubory, adresáři a aplikacemi
- Spolehlivě určí rozdíl mezi zálohováním a archivací a umí nastavit základní parametry obojího
- Zná bezpečnostní prvky v jednotlivých aplikacích
- Ovládá základní typy licencí, zná licenční politiky a neinstaluje software z neznámých zdrojů
- Umí bezpečně provést jednoduché instalace i odinstalace software.
- Chápe význam zabezpečeného připojení, používá digitální podpis

ZÁKLADNÍ ZNALOSTI V OBLASTI SOFTWARE, ZEJMÉNA APLIKACÍ II.

- Žák zná zásady bezpečného používání digitálních technologií včetně tvorby silného hesla a chápe nutnost změny hesla v určitém intervalu
- Zná zásady práce se soubory, adresáři a aplikacemi
- Spolehlivě určí rozdíl mezi zálohováním a archivací a umí nastavit základní parametry obojího
- Zná bezpečnostní prvky v jednotlivých aplikacích a aktivně je používá, umí rozpoznat bezpečný dokument, umí nastavit např. heslo v dokumentu, chápe oběh dokumentu organizací včetně ověření vlastností a autora
- Ovládá základní typy licencí, zná licenční politiky a neinstaluje software z neznámých zdrojů. Chápe omezení, daná bezpečnostními zásadami na síti a dodržuje daná pravidla.
- Chápe význam zabezpečeného připojení, používá digitální podpis

ZÁKLADNÍ ZNALOSTI V OBLASTI SOFTWARE, ZEJMÉNA APLIKACÍ III.

- Žák zná zásady bezpečného používání digitálních technologií včetně tvorby silného hesla a chápe nutnost změny hesla v určitém intervalu. Je si vědom, že vynucené změny hesla s příliš častou frekvencí snižují bezpečnost, dokáže vysvětlit princip tvorby silného hesla a správně jej aplikovat.
- Zná zásady práce se soubory, adresáři a aplikacemi. Dokáže obnovit soubory, zná rizika tohoto kroku v souvislosti s napadením zařízení.
- Spolehlivě určí rozdíl mezi zálohováním a archivací a umí nastavit základní parametry obojího
- Zná bezpečnostní prvky v jednotlivých aplikacích a aktivně je používá, umí rozpoznat bezpečný dokument
- Ovládá typy licencí, zná licenční politiky a neinstaluje software z neznámých zdrojů. Chápe omezení, daná bezpečnostními zásadami na síti a dodržuje daná pravidla. Rozpozná porušení licenčních zásad, nepoužívá nelicencovaný software.
- Chápe význam zabezpečeného připojení, používá digitální podpis

ZÁKLADNÍ ZNALOSTI V OBLASTI KOMUNIKACE

ZÁKLADNÍ ZNALOSTI V OBLASTI KOMUNIKACE I.

- Žák má zažito bezpečné chování s ohledem na možný mallware a zná běžné způsoby detekce. Je schopen identifikovat problém a nahlásit jej správci IT
- Žák dokáže rozlišit soukromou (domácí či pracovní) a veřejnou síť. Zná pravidla pro pohyb na veřejných sítích, pečlivě rozlišuje mezi pracovní a soukromou komunikací (mailem, skupinou, messengerem).
- Žák umí vysvětlit a aplikovat pravidla bezpečné virtuální komunikace. Dokáže rozpoznat rizikovou virtuální komunikaci. Ví, jak podat oznámení při podezření na spáchání trestného činu
- Při pohybu v online světě buduje uvědoměle svoji digitální stopu (například orientuje se v podmínkách přístupu na sociální sítě, zná pravidla zveřejňování informací, ovládá nastavení soukromí na sociálních sítích).
- Žák aktivně aplikuje pravidla hygieny při práci s digitální technikou.
- Žák dokáže analyzovat informace, s nimiž pracuje. Aktivně ověřuje obsah předkládaných sdělení například na stránkách Hoax.cz
- Žák zná základy sociálního inženýrství a podprahových manipulací. Předchází nebezpečným situacím, upozorňuje správce sítě na rizikové momenty a umí tyto techniky rozpoznat.
- Je schopen provést základní poučení u kolegů, rozpozná nevhodné návyky a sám je neakceptuje

ZÁKLADNÍ ZNALOSTI V OBLASTI KOMUNIKACE II.

- Žák má zažito bezpečné chování s ohledem na možný mallware a zná běžné způsoby detekce. Je schopen identifikovat problém a nahlásit jej správci IT
- Žák dokáže rozlišit soukromou (domácí či pracovní) a veřejnou síť. Zná pravidla pro pohyb na veřejných sítích, pečlivě rozlišuje mezi pracovní a soukromou komunikací (mailem, skupinou, messengerem).
- Žák umí vysvětlit a aplikovat pravidla bezpečné virtuální komunikace. Dokáže rozpoznat rizikovou virtuální komunikaci a zná preventivní postupy. Ví, jak podat oznámení při podezření na spáchání trestného činu, zná základní paragrafy trestního zákoníku, týkající se kyberkriminality
- Při pohybu v online světě buduje uvědoměle svoji digitální stopu (například orientuje se v podmínkách přístupu na sociální sítě, zná pravidla zveřejňování informací, ovládá nastavení soukromí na sociálních sítích).
- Žák aktivně aplikuje pravidla hygieny při práci s digitální technikou.
- Žák dokáže analyzovat informace, s nimiž pracuje. Ví, jak se zachovat při nalezení nevhodného obsahu a sám aktivně ověřuje obsah předkládaných sdělení například na stránkách Hoax.cz
- Žák zná základy sociálního inženýrství a podprahových manipulací.
- Rozpozná nevhodné návyky a sám je neakceptuje

ZÁKLADNÍ ZNALOSTI V OBLASTI KOMUNIKACE III.

- Žák má zažito bezpečné chování s ohledem na možný mallware a zná běžné způsoby detekce. Má dovednosti, potřebné pro bezpečný pohyb na síti
- Žák dokáže rozlišit soukromou (domácí či pracovní) a veřejnou síť. Zná pravidla pro pohyb na veřejných sítích, pečlivě rozlišuje mezi pracovní a soukromou komunikací (mailem, skupinou, messengerem).
- Žák umí vysvětlit a aplikovat pravidla bezpečné virtuální komunikace. Dokáže rozpoznat rizikovou virtuální komunikaci a zná preventivní postupy. Ví, jak podat oznámení při podezření na spáchání trestného činu, zná základní paragrafy trestního zákoníku, týkající se kyberkriminality
- Při pohybu v online světě buduje uvědoměle svoji digitální stopu (například orientuje se v podmínkách přístupu na sociální sítě, zná pravidla zveřejňování informací, ovládá nastavení soukromí na sociálních sítích).
- Žák aktivně aplikuje pravidla hygieny při práci s digitální technikou.
- Žák dokáže analyzovat informace, s nimiž pracuje. Ví, jak se zachovat při nalezení nevhodného obsahu a sám aktivně ověřuje obsah předkládaných sdělení například na stránkách Hoax.cz
- Žák zná základy sociálního inženýrství a podprahových manipulací. Aktivně předchází nebezpečným situacím, upozorňuje správce sítě na rizikové momenty a umí se těmto technikám bránit.
- Je schopen provést základní poučení u kolegů, rozpozná nevhodné návyky a sám je neakceptuje. Dokáže vysvětlit rizika, vyplývající ze špatných návyků a nedodržování bezpečnostních pravidel.