Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

5151/2023-NÚKIB-E/630 • BRNO • 1. ČERVENCE 2023

STRATEGICKÁ ANALÝZA

ÚTOKY S VYUŽITÍM KVANTOVÉHO POČÍTAČE MOHOU PROLOMIT SOUČASNÉ ŠIFROVÁNÍ: ŘEŠENÍM JE VČASNÁ A EFEKTIVNÍ IMPLEMENTACE NOVÝCH STANDARDŮ

SHRNUTÍ

- **Vzhledem k limitacím současných počítačů probíhá aktivně vývoj nového typu počítače. Kvantové počítače využívají principy kvantové mechaniky, přičemž ve svých výkonech mohou výrazně překonat současné klasické mikrotranzistorové počítače. Jejich schopnosti slibují průlom v mnoha vědeckých odvětvích, nicméně zároveň představují hrozbu pro většinu současných metod šifrování.**
- **Kvantové počítače schopné útoků, které překonají současné šifrování (tzv. kryptograficky relevantní kvantové počítače), mohou být k dispozici v horizontu 5–15 let. Škodliví aktéři mohou tyto schopnosti zneužít k útokům, které budou cílit na odcizení dat, či demonstrativním útokům s cílem podlomit důvěru v určité organizace a služby (např. vládní orgány, internetové bankovnictví atd.).**
- **V současnosti probíhá vývoj nových šifrovacích standardů, které kvantovým počítačům odolají. Ty budou dostupné velmi pravděpodobně (75–85 %) dříve než tzv. kryptograficky relevantní kvantové počítače. Klíčová bude jejich efektivní a včasná implementace, potažmo schopnost rychle přijímat případné aktualizace.**
- **Organizace by se měly začít připravovat na přechod na postkvantové šifrování a udržovat tzv. kryptografickou pružnost, tedy schopnost rychle kombinovat, upravovat a měnit používané kryptografické algoritmy.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací partnerů NÚKIB, z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace.

Jedním z mnoha možných praktických využití unikátních jevů kvantové mechaniky jsou kvantové počítače. Tyto počítače mohou v horizontu 5–15 let svými výkony dalece překonat současné počítače a přinést průlomy v mnoha odvětvích lidské činnosti. Schopnosti kvantových počítačů ovšem zároveň ohrožují bezpečnost dnešních šifrovacích standardů.

VÝVOJ KVANTOVÝCH POČÍTAČŮ NYNÍ POSTUPUJE RYCHLE, ALE JE OBTÍŽNĚ PŘEDVÍDATELNÝ

Kvantové počítače prochází intenzivním vývojem, a přitahují velké investice.[1] Přesto je obtížné stanovit jasný trend jejich budoucího vývoje. Dnešní kvantové počítače zatím představují experimentální zařízení, jež překonávají současné mikrotranzistorové počítače jen ve velmi specifických úlohách (viz Box 1).

Box 1: Kvantová nadřazenost a kvantová výhoda

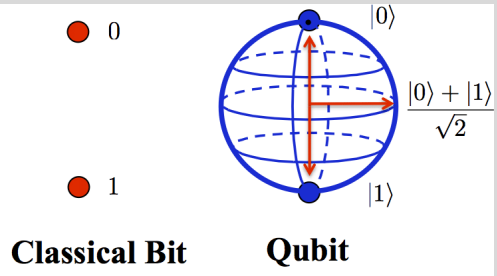
Kvantová nadřazenost představuje hranici, kdy kvantové počítače podají výsledky, kterých by nebylo možné dosáhnout se standardním binárním mikrotranzistorovým počítačem. Ačkoliv dnes je již tato hranice považována za překonanou (poprvé zřejmě společností Google v roce 2019), zatím se jedná zpravidla o specifické úkoly, často vytvořené na míru pro demonstraci schopností kvantových počítačů. Současné úsilí je tak zaměřeno na dosažení tzv. kvantové výhody, tedy bodu, kdy bude výhodnější použít kvantový počítač k plnění konkrétního praktického úkolu, namísto klasického binárního počítače.

Je téměř jisté (90–100 %), že vývoj kvantových počítačů bude dále intenzivně probíhat a dospěje do bodu (tzv. kryptograficky relevantní kvantový počítač), kdy budou představovat vážnou hrozbu pro kybernetickou bezpečnost. [3] **Je však těžké přesněji odhadnout, v jakém časovém horizontu se tak stane, neboť vývoj naráží na řadu výzev. Je téměř jisté (90–100 %), že to nebude dříve než za pět let.**

Box 2: Bit vs. qubit a superpozice

Dnešní počítače fungují v tzv. binární soustavě. Informace, které jsou zpracovávány procesory, mají hodnoty 1 nebo 0, tedy ANO nebo NE, s tím, že jednotka informace (tzv. bit) může mít jenom jednu z těchto hodnot.[2] V kvantových počítačích je jednotkou informace qubit (čti *kjúbit*). Jedná se o částici, která může existovat v obou stavech zároveň (tzv. superpozice), a teoreticky tak nést dvojnásobek informací. Hlavní silou qubitů je ovšem možnost jejich kombinací. Díky superpozici mohou již dva qubity představovat osm různých kombinací (tedy informací) a tento počet narůstá geometrickou řadou s každým dalším qubitem. I relativně malé množství tak může nést v porovnání s bity obrovské množství dat a v rámci jedné operace vyřešit výrazně složitější matematické úkoly.

Obr. 1: Rozdíl mezi bitem a qubitem



První velkou výzvou v rozvoji kvantových počítačů je navýšení počtu fyzických qubitů, tedy jednotlivých kvantových bitů přenášejících a zpracovávajících informace (viz Box 2). Druhou výzvou je pak navýšení počtu logických qubitů, tedy qubitů, které plní svou funkci v daném kvantovém algoritmu. Nyní se pracuje jak na možnosti navýšení množství fyzických qubitů nebo snížení jejich chybovosti, tak na algoritmech s opravným kódem, které zvládnou pracovat s chybovostí qubitů.[4]

Experimentuje se s různými typy kvantových počítačů (např. supravodivé, na bázi fotonů, křemíkové atd.), které mají různé vlastnosti. [5] Výzkum kvantových počítačů je tak v současnosti hledáním možných cest, jimiž by se vývoj mohl ubírat. Ve chvíli, kdy dojde k prosazení konkrétních osvědčených technologií a procesů, může být jejich vývoj velmi výrazně urychlen. Jako analogie se nabízí například objev integrovaného obvodu v roce 1958 a jeho dopad na následný rapidní vývoj výpočetní techniky.

KVANTOVÉ ÚTOKY MOHOU BÝT SKRYTÉ I DEMONSTRATIVNÍ, BUDOU CÍLIT NA CITLIVÁ DATA ČI KLÍČOVÉ SLUŽBY

Útoky vedené kvantovým počítačem proti šifrování mohou ohrozit veškeré současné kryptografické standardy pro asymetrické šifrování a digitální podpisy. [6] **Kvantové útoky, jež mohou v budoucnu nastat, pak mohou být buď skryté (snažící se maskovat skutečnost, že útočník disponuje kryptograficky relevantním kvantovým počítačem), nebo může jít o útoky, které naopak mají za cíl demonstrovat schopnosti kvantového počítače.** Nelze vyloučit (25–50 %) ani útoky pouze předstírající provedení skrze kvantový počítač (viz Box 3).

Cílem skrytých útoků, pokud k nim dojde, budou velmi pravděpodobně (75–85 %) organizace, které disponují vysoce citlivými daty, např. ministerstva či společnosti s cenným know-how, jako jsou vyspělé technologie či vojenská výroba. Primární snahou bude získat nejenom citlivé informace, nýbrž v ideálním případě je získat takovým způsobem, že oběť nebude vědět o jejich kompromitaci (tj. bude například zachycovat šifrovanou komunikaci mezi pobočkami dané organizace a s pomocí kvantového počítače bude schopen tuto komunikaci číst bez vědomí oběti).

Demonstrativní útoky naopak představují útoky, kde útočník kromě samotného kvantového počítače pracuje i s psychologickým prvkem. Jejich účelem je ukázat schopnosti odpovědného aktéra a narušit důvěru v určitý systém, službu, společnost či stát. Klíčovým faktorem daného útoku by pravděpodobně (55–70 %) byla snaha zveličovat reálné schopnosti kvantového počítače s cílem vyvolat nedůvěru, případně až paniku u široké veřejnosti, jež si nebude vědoma různých omezení kvantových útoků. **Pokud dojde například k úspěšnému kvantovému útoku na elektronické bankovnictví, u širší veřejnosti může**

nastat obava z narušení důvěrnosti nebo integrity těchto služeb, přestože daný útok může být pouze méně závažný a jeho opakování mitigovatelné. Takový útok by navíc mohl být následně podpořen dalšími prostředky, například dezinformačními kampaněmi. Je proto třeba brát v potaz, že útok kvantovým počítačem může být jen jedním z prvků rozsáhlé kampaně vyspělého aktéra, kdy se efekt kvantového útoku nemusí odvíjet pouze od technických faktorů.

Cíle demonstrativního útoku mohou být totožné jako v případě útoků diskrétních, ale pravděpodobně (55–70 %) budou vedeny spíše proti organizacím nebo službám, v nichž figuruje výrazný prvek důvěry. Může se tak jednat například o bankovní instituce, vládní systémy pro komunikaci s občany, volební systémy nebo zdravotní instituce. Vhodný cíl takového útoku mohou hypoteticky představovat i kryptoměny. **Ačkoliv faktický rozsah a dopad útoku nemusí být rozsáhlý, psychologický aspekt narušení důvěry v tento druh institucí a služeb může mít dalekosáhlé dopady na stabilitu a bezpečnost společnosti.** Možným cílem takového útoku může být také snaha o podrytí bezpečné a efektivní implementace šifrování, které je odolné kvantovým počítačům (viz Box 3).

BOX 3: Rizika urychlené implementace postkvantového šifrování

Aby šifrovací algoritmy plnily svůj účel, musí být řádně implementovány. V případě, že jsou implementovány špatně, mohou být pro útočníka překonatelné, přestože jsou ze své podstaty v současnosti nepřekonatelné.

Toho by se mohl pokusit útočník s kvantovým počítačem využít. Demonstrativní útok by mohl eventuálně spustit vlnu překotné implementace postkvantového šifrování. Poté by pak mohla vzniknout řada zranitelností, které by útočník mohl zneužít konvenčními metodami, aniž by využil kvantový počítač.

K vyvolání tohoto efektu by navíc mohl útočník použití kvantového počítače jen předstírat. Pokud by útočník dokázal obejít šifrování pomocí jiné neznámé zranitelnosti a zároveň přesvědčit světovou kyberbezpečnostní komunitu, že tak učinil pomocí kvantového počítače, tak by stejně tak mohl spustit vlnu ukvapené implementace postkvantového šifrování.

K tomu, aby se útočník pokusil o takový demonstrativní útok, nahrává současná situace. Probíhající vývoj a prvotní implementace kryptografických algoritmů odolných vůči kvantovým počítačům totiž umožní kvantovým útokům v budoucnu zabránit (viz následující kapitola). **Zatímco diskrétní útoky budou moci dále probíhat alespoň vůči dříve odcizeným nedostatečně zašifrovaným datům (viz Příloha 1), čas, kdy může útočník využít kvantový počítač pro demonstrativní útok, se krátí.** Bude-li škodlivý aktér chtít využít svůj kvantový počítač ofenzivně, bude tak zřejmě muset učinit relativně brzo. A v případě, že jeho kvantový počítač nebude schopen provést demonstrativní útok velkého rozsahu, bude pravděpodobně (55–70 %) případné nedokonalosti kvantového počítače kompenzovat psychologickým aspektem a s ním spjatým výběrem vhodného cíle.

POSTKVANTOVÉ ŠIFROVÁNÍ PŘINESE EFEKTIVNÍ OCHRANU PŘED KVANTOVÝMI ÚTOKY

V době, kdy budou kvantové počítače schopné prolamovat současné kryptografické standardy, budou již téměř jistě (90–100 %) existovat nové standardy, které kvantovým počítačům odolají. Nyní se aktivně pracuje na metodách zajištění tzv. postkvantové bezpečnosti, tedy šifrovacích algoritmů schopných odolat útoku kvantového počítače a nevyžadujících výrazně větší výpočetní výkon než současné šifrovací standardy.[7] Americký Národní institut pro standardizaci a technologii (NIST) dokončuje mezinárodní soutěžní program, ze kterého má vzejít nový standard odolný vůči kvantovým útokům.[8]

Aktuálně nejslibnějším kandidátem pro dosažení šifrování odolného kvantovým počítačům je kryptografie založená na mřížkách (lattice-based cryptography).[9] Ta využívá výrazně odlišné matematické principy než současné šifrovací metody, přičemž není zranitelná vůči kvantovým algoritmům. Tyto matematické operace jsou zároveň zpracovatelné i se současnými běžně dostupnými počítači. **Jakmile budou postkvantové algoritmy ze soutěže NIST úspěšně dokončeny, budou představovat efektivní ochranu před kvantovými útoky.**

Kromě postkvantového šifrování je účinným ochranným prostředkem též kvantová výměna klíčů. Tato technologie využívá podobné fyzikální jevy jako kvantový počítač, konkrétně superpozici, k bezpečnému přenosu šifrovacích klíčů, který je odolný i vůči kvantovému počítači. Toto řešení je ovšem technologicky i finančně velmi náročné (viz Box 2 a Příloha 2).

IMPLIKACE: ZÁSADNÍ JE ŘÁDNÁ A VČASNÁ IMPLEMENTACE

Možnosti implementace postkvantové kryptografie v současnosti stojí primárně na dokončení soutěže NIST a posléze na tom, kdy tato kryptografická řešení začnou nabízet relevantní dodavatelé (např. hlavní poskytovatelé cloudových služeb). Ačkoliv finalisté soutěže NIST jsou již známí a jejich řešení je možné teoreticky implementovat, bude vhodné vyčkat, než bude soutěž NIST dokončená a než bude připravena standardizovaná implementace, a to vzhledem k rizikům, která z neodborné implementace plynou. K tomu by mělo dojít v horizontu několika let.

Řádná implementace šifrovacích standardů je klíčová pro kyberbezpečnost. Špatně implementované kryptografické prostředky mohou vést k narušení integrity a důvěryhodnosti dat, přestože samotné šifrování je dostatečně odolné. U postkvantové kryptografie to znamená, že v případě špatné implementace mohou být útočníkovi dostupná citlivá data, a to i bez použití kvantového počítače.

Dalším faktorem je, že postkvantové šifrování musí odolat jak kvantovým útokům, které v současnosti nejsou proveditelné, tak zároveň ostatním dnes používaným formám útoků nevyžadujícím kvantový počítač. Vzhledem k této komplexitě je možné, že s postupem času budou odhaleny zranitelnosti (vůči kvantovým i konvenčním útokům), včetně implementačních, jež bude třeba opravit, tudíž nelze vyloučit (25–50 %) neočekávané komplikace při následné implementaci postkvantových standardů. **Je pravděpodobné (55–70 %), že v případě postkvantového šifrování bude potřeba častějších změn v používaných šifrovacích prostředcích, než tomu bylo doposud.**

DOPORUČENÍ: KLÍČOVÁ BUDE KRYPTOGRAFICKÁ PRUŽNOST

Hlavním milníkem pro kybernetickou bezpečnost v kontextu kvantových počítačů bude dokončení soutěže NIST a následná implementace vítězných algoritmů do nabídky hlavních dodavatelů IT řešení. Přestože je možné vyčkávat do tohoto bodu, je klíčové být následně připraven na co nejrychlejší a nejhladší implemetaci.

Pro úspěšnou implementaci nejen nových šifrovacích standardů, ale i jakýchkoli dalších prvků kybernetické bezpečnosti, by měl být používán aktuální software a pokud možno i hardware.

Klíčovým aspektem pro úspěšnou implementaci kvantových počítačů bude koncepce kryptografické pružnosti, tedy schopnosti rychle měnit či kombinovat šifrovací standardy.

V praxi kryptografická pružnost znamená znát všechny algoritmy, délky klíčů, kryptografické knihovny a protokoly používané v aplikacích, které organizace využívá, a být schopen je neprodleně a efektivně aplikovat v případě potřeby změny.

Ačkoliv soutěž NIST ještě není zcela dokončená, vítězné algoritmy jsou již nyní známy, přičemž je možné je na vlastní zodpovědnost implementovat. S takovým postupem se ovšem pojí rizika, že algoritmy budou ještě upraveny a bude třeba je opět složitě měnit. Jisté riziko spočívá také v potenciálně chybné implementaci jako takové.

V rámci co nejrychlejší implementace postkvantového šifrování je vhodné jej kombinovat s jinou osvědčenou konvenční kryptografií.

PŘÍLOHA 1: HROZBA ZPĚTNÉHO PROLOMENÍ: V MINULOSTI ODESLANÉ INFORMACE MOHOU BÝT V BUDOUCNU DEŠIFROVÁNY

Významnou hrozbou využití kvantových počítačů, kterou je třeba reflektovat, je tzv. zpětné prolomení. **Vývoj a aplikace šifrované komunikace, jež obstojí proti kvantovému počítači, totiž zpětně nepokryjí data odeslaná v minulosti, kdy ještě nebylo využíváno dostatečně odolné šifrování, a útočník si je uložil k pozdějšímu prolomení.** V případě státních aktérů, kteří budou schopni vyvinout efektivní kvantový počítač, se může daný soubor šifrované komunikace stát zpětně prolomitelným. Pro zpětné prolamování mají nejlepší předpoklady aktéři, kteří mají nebo mohou mít kontrolu nad síťovou infrastrukturou a díky tomu disponovat širokými možnostmi způsobů zisku dat.

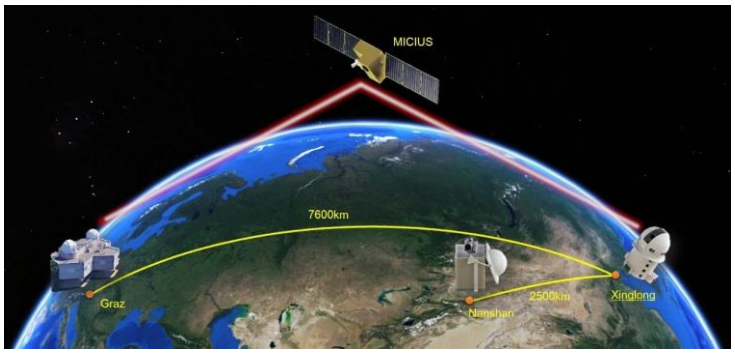
Přestože nástup kryptograficky relevantních kvantových počítačů není možné téměř jistě (90–100 %) očekávat za dříve než pět let, mnoho citlivých informací má dlouhodobou relevanci. Jejich rozklíčování i po několika letech může přivodit původním adresátům informací značné škody a rizika. **S informacemi zachycenými pro pozdější kvantové prolomení již není možné cokoli udělat a není možné je nijak zpětně aktualizovat na bezpečnější šifrovací standard.**[10] Příkladem může být šifrovaná komunikace ve zdravotnictví. Útočník může například zpětně rozšifrovat citlivá zdravotní data významných státních činitelů, která si mezi sebou skrze šifrovanou komunikaci sdílela zdravotnická zařízení. **Je proto třeba implementovat co nejdříve kryptografické standardy, které kvantovým útokům odolají, a do té doby reflektovat skutečnost, že odesílané informace nemusí být zcela v bezpečí.**

PŘÍLOHA 2: KVANTOVÁ DISTRIBUCE KLÍČŮ

Kvantová distribuce klíčů (Quantum Key Distribution – QKD) je metoda zabezpečení asymetrické šifrované komunikace, jež ke svému fungování využívá kvantové jevy, konkrétně fenomén superpozice. Jeden z účastníků komunikace nejprve pošle druhému fotony ve stavu superpozice. S ohledem, že změření stavu fotonu vede ke zhroucení superpozice, je možné zjistit, zda poslané fotony po cestě někdo nezachytil a nepřečetl. Hypoteticky tímto způsobem lze dosáhnout bezprecedentní míry bezpečnosti. Takto zabezpečená komunikace nespoléhá na technologické limity počítačů, ale na fyzikální principy. Komunikace zabezpečená skrze QKD je proto v bezpečí i před útokem vedeným kvantovým počítačem.

Ačkoliv je QKD prakticky již fungující technologií, v současnosti naráží na mnoho překážek bránících jejímu masovějšímu použití (např. omezená vzdálenost v optickém vlákně, náročnost posílání fotonů přes satelit, potřeba dedikované infrastruktury atd.). EU pracuje na páteřní kvantově zabezpečené síti, jež se v prvotní fázi zaměří na strategické instituce a nejkritičtější komunikaci. Ačkoliv lze očekávat, že QKD čeká v horizontu dvaceti a více let velký rozvoj, v současnosti není dostatečně dostupnou a rozvinutou alternativou na to, být efektivní ochranou před kvantovými útoky.

Obr. 2: Schéma kvantové výměny klíčů pomocí laserů a satelitu na orbitě



Zdroj: phys.org

ZDROJE

[1] Quantum Technology Monitor. 2022. McKinsey & Company. quantum-technology-monitor.pdf (mckinsey.com)
[2] What is quantum computing? 2023. Caltech. What Is Quantum Computing? | Caltech Science Exchange
[3] Quantum Computing and Post-Quantum Cryptography FAQ. 2022. National Security Agency. Quantum_FAQs_20210804.PDF (defense.gov)
[4] ROBINSON, Dan. 2023. Google claims milestone in quantum error correction. The Register. Google claims milestone in quantum error correction • The Register
[5] What is Quantum computing? 2023. Amazon Web Services. What is Quantum Computing? - Quantum Computing Explained - AWS (amazon.com), University of New south Wales. 2022. Major Breakthrough As Quantum Computing in Silicon Hits 99% Accuracy. SciTech Daily. Major Breakthrough As Quantum Computing in Silicon Hits 99% Accuracy (scitechdaily.com)
[6] TEIK, Guan Tan, Szalachowski Pawel, ZHOU, Jianying. 2021. Challenges of Post-Quantum Digital Signing in Real-world Applications: A Survey. Singapore University of Technology and Design. 1374.pdf (iacr.org)
[7] MATEEN, Abdul. 2021. What is post-quantum cryptography?. Educative. What is post-quantum cryptography? (educative.io)
[8] Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. 2022. NIST. NISTIR 8413, PQC Project Third Round Report | CSRC
[9] A Guide to Post-Quantum Cryptography. 2022. Trail of Bits. A Guide to Post-Quantum Cryptography | Trail of Bits Blog
[10] GRIMES, Roger. 2. 8. 2018. How quantum computers will destroy and (maybe) save cryptography. Computerworld. computerworld.com.au/article/644704/how-quantum-computers-will-destroy-maybe-save-cryptography

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP: RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP: AMBER**	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
Oranžová **TLP: AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
Zelená **TLP: GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP: CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit / Reálná možnost	*25–50 %*
Nepravděpodobně	*15–20 %*
Velmi nepravděpodobně	*0–10 %*