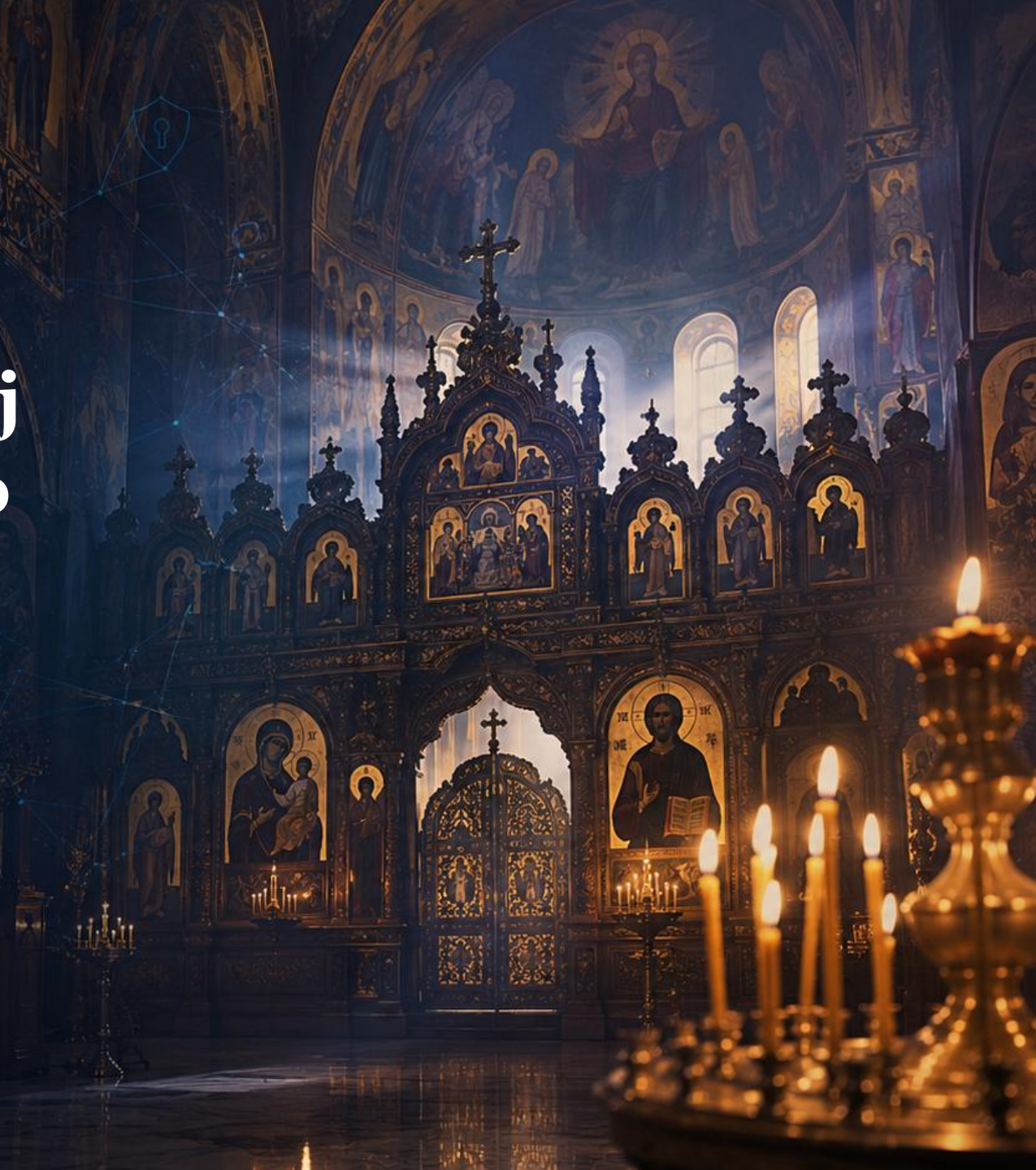
WYKŁAD - 60 MINUT

Cyberbezpieczeństwo w przestrzeni parafialnej Kościoła prawosławnego

Od ochrony danych wiernych do odporności kancelarii, finansów i komunikacji parafialnej.

Autor: dr Tomasz Wierzchowski
Materiał dydaktyczny

2026



STRUKTURA

Mapa wykładu

1. Parafia jako ekosystem informacji
2. Dane wiernych i odpowiedzialność zaufania
3. Najczęstsze cyberzagrożenia
4. Kancelaria, media społecznościowe i finanse
5. Minimalny standard oraz procedura incydentu

Cel: przełożyć cyberbezpieczeństwo z języka technicznego na język praktycznej odpowiedzialności parafii.

PUNKT WYJŚCIA

Teza główna

Cyberbezpieczeństwo parafii nie jest luksusem technicznym, lecz formą ochrony człowieka, jego prywatności, godności i zaufania do wspólnoty.

CHRONIMY

dane

BUDUJEMY

zaufanie

WZMACNIAMY

wspólnotę

W praktyce: nie klikamy bez namysłu, nie udostępniamy danych bez potrzeby, sprawdzamy przelewy i reagujemy szybko na incydenty.

Parafia jako ekosystem informacyjny

- kancelaria parafialna: dokumenty, e-mail, zaświadczenia, księgi
- komunikacja duszpasterska: telefon, SMS, komunikatory, grupy
- internet: strona www, profile społecznościowe, transmisje
- finanse: konto bankowe, faktury, darowizny, zbiórki
- edukacja i wolontariat: dzieci, młodzież, osoby starsze

Pytanie kontrolne: co mamy, co chronimy, kto ma dostęp i co robimy, gdy coś pójdzie źle?

DANE

Dane wiernych: wymiar prawny i duszpasterski

- informacje o życiu religijnym i sakramentalnym
- dane rodzin, dzieci, osób starszych i potrzebujących
- prośby o pomoc, informacje o chorobie i sytuacji życiowej
- adresy, telefony, e-maile, zgody, listy uczestników
- odpowiedzialność nie tylko formalna, ale także moralna

RODO art. 91 pozwala Kościołom i związkom wyznaniowym stosować własne szczegółowe zasady ochrony danych, jeżeli spełniają wymogi zgodności z RODO.

Najgroźniejszy punkt ataku: człowiek

- phishing: fałszywy bank, urząd, diecezja, dostawca lub platforma społecznościowa
- spear-phishing: wiadomość przygotowana specjalnie pod proboszcza, skarbnika lub kancelarię
- vishing i smishing: telefon lub SMS z presją czasu
- fałszywa faktura albo „pilna” zmiana numeru rachunku
- deepfake: głos, obraz lub tekst podszywający się pod osobę zaufania

Reguła: każdą wiadomość z presją czasu traktujemy jako potencjalne ryzyko i weryfikujemy drugim kanałem.

Typowe incydenty w parafii

01	**Przejęcie profilu**	fałszywa zbiórka, zmiana ogłoszeń, utrata reputacji
02	**Ransomware**	zaszyfrowane dokumenty kancelarii i brak kopii zapasowej
03	**Oszustwo fakturowe**	podmieniony numer konta przy remoncie lub zakupie
04	**Wyciek danych**	lista dzieci, wolontariuszy lub osób potrzebujących pomocy
05	**Fałszywy autorytet**	podszycie pod duchownego, radę parafialną albo bank

Wspólny mianownik: sprawca wykorzystuje zaufanie, pośpiech i brak jasnych procedur.

STANDARD

Pięć zasad cyberbezpiecznej parafii

01 minimum dostępu

02 silne logowanie i 2FA

03 kopie zapasowe

04 ostrożna komunikacja

05 procedura incydentu

Nie chodzi o drogi system, ale o powtarzalne zachowania: mniej dostępu, więcej weryfikacji, kopie i szybka reakcja.

KANCELARIA

Kancelaria parafialna: punkt szczególnego ryzyka

- oddzielny komputer i oddzielna poczta do spraw parafialnych
- automatyczna blokada ekranu, aktualizacje, antywirus
- dokumenty i wydruki poza zasięgiem osób postronnych
- niszczarka dla błędnych wydruków i notatek z danymi
- zasada czystego biurka i czystego ekranu

Kancelaria to nie tylko miejsce pracy. To przestrzeń poufności duszpasterskiej i administracyjnej.

KOMUNIKACJA

Media społecznościowe i transmisje nabożeństw

Administratorzy imiennie wskazani, z dostępem odbieranym po zakończeniu funkcji

Zdjęcia szczególna ostrożność przy dzieciach, osobach chorych i potrzebujących

Transmisje kamera nie może ujawniać spowiedzi, rozmów, dokumentów ani sytuacji kryzysowych

Profil parafii 2FA, kontrola ról, brak udostępniania haseł przez komunikatory

Publikacja jest formą odpowiedzialności: nie wszystko, co można sfotografować, powinno być pokazane publicznie.

FINANSE

Finanse parafii: ochrona środków powierzonych

- większy przelew zawsze potwierdzony drugim kanałem
- zmiana numeru rachunku wykonawcy wymaga osobnej weryfikacji
- zbiórki tylko przez oficjalne kanały parafii
- stały, publicznie weryfikowalny numer konta do darowizn
- zasada dwóch par oczu przy płatnościach i fakturach

To nie brak zaufania. To ochrona wspólnoty i osób odpowiedzialnych za majątek parafii.

REAKCJA

Procedura incydentu: pierwsze 30 minut

1	**Zatrzymaj**	nie klikaj dalej, nie wykonuj kolejnych przelewów
2	**Zabezpiecz dowody**	zrzut ekranu, e-mail, numer telefonu, link, data
3	**Powiadom**	proboszcz, osoba techniczna, skarbnik lub administrator
4	**Odłącz i zmień**	hasła, dostęp do kont, sesje, urządzenia
5	**Oceń i zgłoś**	dane osobowe, bank, CERT, policja, właściwy organ kościelny

Najgorszą reakcją jest wstyd i milczenie. W cyberbezpieczeństwie szybkość reakcji ogranicza szkodę.

CHECKLISTA

Minimalny standard do wdrożenia od zaraz

- ✓ adres e-mail parafii
- ✓ menedżer haseł lub bezpieczny rejestr
- ✓ 2FA: poczta, bank, Facebook, YouTube
- ✓ kopie zapasowe dokumentów
- ✓ lista osób z dostępem
- ✓ weryfikacja przelewów drugim kanałem
- ✓ zasady publikacji zdjęć i transmisji
- ✓ czysty ekran i czyste biurko
- ✓ krótka procedura incydentu
- ✓ szkolenie raz w roku

Cyberbezpieczna parafia chroni dane, zaufanie i wspólnotę.

Źródła i podstawy

• CERT Polska, Raport roczny 2025 oraz materiały edukacyjne dotyczące phishingu i bezpiecznych haseł.

• ENISA, Threat Landscape 2025 - zagrożenia: phishing, socjotechnika, ransomware, AI-enabled attacks.

• Urząd Ochrony Danych Osobowych: informacje o współpracy Prezesa UODO z KIODO Polskiego Autokefalicznego Kościoła Prawosławnego.

• RODO, art. 91 - szczególne zasady ochrony danych w Kościołach i związkach wyznaniowych.

• Dobre praktyki: minimalny dostęp, 2FA, kopie zapasowe, weryfikacja płatności, procedura incydentu.

Autor opracowania: dr Tomasz Wierzchowski