Router Nieuprawniony dostęp do panelu administracyjnego poprzez ataki brute force lub domyślne dane logowania. Atak zewnętrzny - zagrożenie techniczne Atak typu Denial of Service (DS) blokujący dostęp do sieci. Atak zewnętrzny - zagrożenie techniczne 1.4 Infekcja malware: instalacja żłośliwego oprogramowania danych. Podszywanie się pod router (ARP spoofing) w celu przechwycenie danych. Atak wewnętrzny - zagrożenie techniczne. Atak wewnętrzny - zagrożenie techniczne. Atak zewnętrzny - zagrożenie techniczne. Podszywanie się pod router (ARP spoofing) w celu przechwycenia danych. Atak wewnętrzny - zagrożenie techniczne. Atak wewnętrzny - zagrożenie techniczne. Podszywanie się pod router (ARP spoofing) w celu przechwycenia danych. Atak wewnętrzny - zagrożenie techniczne. Atak wewnętrzny - zagrożenie danych przezethwycenie danych przechwycenie danych przesyłanych oprogramowanie (np. botnet) instalowane na	, , ,
Nieuprawniony dostęp do panelu administracyjnego poprzez ataki brute force lub domyślne dane logowania. 1.2 Atak DoS: przeciążenie serwera techniczne 1.3 Atak ARP spoofing: podszywanie się pod router (ARP spoofing) w celu przechwycenia danych. 1.4 Infekcja malware: instalacja złośliwe oprogramowanie (np. botnet) 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie utechniczne. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.4 Regularne aktualizacje firmware'u. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.4 Regularne aktualizacje firmware'u. 1.4 Regularne aktualizacje firmware'u. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.4 Regularne aktualizacje firmware'u. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.4 Regularne aktualizacje firmware'u. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.4 Regularne aktualizacje firmware'u. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć. 1.5 kamanie hasła Wi-Fi Atak wewnętrzny - zagrożenie danych przez sieć.	a. ustawień routera.
dostęp do panelu administracyjnego poprzez ataki brute force lub domyślne dane logowania. 1.2 Atak DoS: przeciążenie serwera 1.3 Atak ARP Atak typu Denial of Service (DoS) blokujący dostęp do sieci. Atak zewnętrzny - zagrożenie techniczne 1.4 Infekcja malware: instalacja złośliwego oprogramowania danych. Podszywanie się pod router (ARP spoofing) w celu przechwycenia danych. Atak wewnętrzny - zagrożenie techniczne. Skutek: Utrata kontroli nad routerem, potencjalne przechwycenie danych przezysłanych oprogramowania (np. botnet) 1.1 Złamanie hasła: metodą brute force, metodą swietowa metodą brute force, metodą stowate metodą brute force, metodą słowikową 1.2 Atak DoS: przeciążenie serwera 1.3 Atak ARP spoofing: podszywanie się pod urządzenia sieciowe 1.4 Infekcja malware: instalacja złośliwego oprogramowania 1.3 Włączenie zabezpieczeń ARI Segmentacja siec Monitorowanie i filtrowanie ruchu ARP. 1.4 Infekcja malware: instalacja złośliwego oprogramowania 1.5 Łamanie hasła Wi-Fi: przechwycenie danych przesyłanych oprogramowanie (np. botnet) 1.6 Vatak DoS: przeciążenie serwera 1.7 Izmiana domyślny danych pogowania włączenie uwierzytelniania dwusktadnikoweg Regularna aktualizacja firmware'u. 1.2 Implementacja filtrów i limitów połączeń. Korzystanie z usłu dostawców oferujących ochronę przed Do Monitorowanie ruchu sieciowego oprogramowania 1.3 Atak ARP 1.4 Infekcja malware: instalacja złośliwego oprogramowania 1.5 Łamanie hasła Wi-Fi: Przechwycenie danych przesyłanych oprogramowanie (np. botnet)	a. ustawień routera.
routerze w celu ataków na inne sieci lub urządzenia. Atak zewnętrzny i wewnętrzny — zagrożenie techniczne. Nieautoryzowany dostęp do konfiguracji sieci bezprzewodowej poprzez słabe hasło Wi-Fi.	pod kątem nieautoryzowanyc h prób logowania. Testy penetracyjne. 1.2 Monitorowanie ruchu sieciowego. Regularne testy odporności na ataki DoS. Weryfikacja logów połączeń. 1.3 Regularny audyt sieci pod kątem ataków ARP. Testy bezpieczeństwa sieci. Weryfikacja logów ARP. 1.4 Regularne skanowanie pod kątem złośliwego oprogramowania. Weryfikacja aktualności firmware'u. Monitorowanie ruchu sieciowego. 1.5 Audyt ustawień sieci bezprzewodowej. Weryfikacja siły hasła Wi-Fi. Testy penetracyjne sieci bezprzewodowej.

USOS Nieautoryzowany dostęp do kont studentkó lub pracowników poprzez ataki phishingowe lub brute force. 2.2 Atak DoS: przeciążenie serwera 2.2. Atak DoS: przeciążenie serwera 2.2. Atak DoS: przeciążenie serwera 2.2. Ochrona DDOS od dostawców ustug. Regularne audyty bezpieczeństwa. 2.2. Regularne testy penetracyjne, weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów dostawców ustug. Redundancja serwerów. Monitorowanie wydajności systemu. Analiza locydentów dostawców ustug. Sobienia dła administracyjnych. Sydrowanie danych w bazie danych w bazi								
USOS Nieautoryzowany dostęp do kont studentkó lub pracowników poprzez ataki phishingowe lub brute force. 2.2 Atak DoS: przeciążenie serwera 2.2. Atak DoS: przeciążenie serwera 2.2. Atak DoS: przeciążenie serwera 2.2. Ochrona DDOS od dostawców ustug. Regularne audyty bezpieczeństwa. 2.2. Regularne testy penetracyjne, weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów bezpieczeństwa. 2.2. Regularne testy becjążeniow. Weryfikacja i analiza licydentów dostawców ustug. Redundancja serwerów. Monitorowanie wydajności systemu. Analiza locydentów dostawców ustug. Sobienia dła administracyjnych. Sydrowanie danych w bazie danych w bazi	System			5	4	4		
studentów lub pracowników poprzez ataki phishingowe lub brute force. 2.3 Modyfikacja danych: falszowanie rekchniczne i organizacyjne. Ataki typu Denial of Service (Dos) uniemozliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny- zagrożenie techniczne, Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjne. Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowana cosyl (no, zatali SQL injection). Atak zewnętrzny- zagrożenie techniczne i organizacyjne. Vierwie de danych akademickich (ocen, zapisów kursów) przez użytkowaników z uprawnieniami administracyjnymi. Atak wewnętrzny- zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (no, zatali SQL injection). Atak zewnętrzny- zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu i pracowników przez nieautoryzowane osoby (no, zatali SQL injection). Atak zewnętrzny- zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu i pracowników przez nieautoryzowane osoby (no, zatali SQL injection).	studencki	Nieautoryzowany	2.1 Złamanie hasła:				2.1. Uwierzytelnianie	2.1. Monitorowanie
pracowników poprzez ataki phishingowe lub brute force. Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Atak typu Denial of Service (DoS) uniemożliwiające korzystanie z utrata krytycznych wzagrożenie techniczne. Atak zewnętrzny-zagrożenie techniczne, organizacyjne. Atak zewnętrzny-zagrożenie techniczne. Nieautoryzowana modyfikacji adanych sakademickich (ocen, zaptśów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak wwnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lutrata krytyza powie w przez wykownikow przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.	USOS	dostęp do kont	phishing, brute force				dwuskładnikowe.	logów dostępu.
poprzez ataki phishingowe lub brute force. Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Atak itypu Deniał of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Nieautoryzowana modyfikacja danych akademickich (zoen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnyn. Atak wewnętrzny - zagrożenie techniczne i organizacyjne, Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne, Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne, Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne, Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne, Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection: Utrata danych w wyniku awarii sprzętu ibu oprogramowania.		studentów lub					Edukacja użytkowników	Regularne testy
phishingowe lub brute force. 2.3 Modyfikacja danych: falszówanie rekordów zagrożenie akademickich corporamowania. 2.4 Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Ataki typu Deniał of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny-zagrożenie techniczne. Mieutoryzowana modyfikacja danych akademickich (ocen, zapisów kurśwó) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny-zagrożenie techniczne i organizacyjne. Przechwycenie danych w wymiku awanii sprzętu lub oprogramowania.		pracowników	2.2 Atak DoS:				na temat phishingu.	penetracyjne.
brute force. Atak zewnętrzny- zagrożenie techniczne i organizacyjne. Ataki typu Denial of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny- zagrożenie techniczne. Nieautoryzowana modyfikacji adanych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny- zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny- zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		poprzez ataki	przeciążenie serwera				Regularne audyty	Weryfikacja i analiza
danych: falszowanie rekordów akademickich techniczne i organizacyjne. Ataki typu Denial of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny zagrożenie techniczne. Nieautoryzowana modyfikacji danych osobowych studentów i przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny zagrożenie techniczne i organizacyjne. Przechwycenie danych w sobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny zagrożenie techniczne i organizacyjne zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny zagrożenie techniczne i organizacyjne zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		phishingowe lub					bezpieczeństwa.	incydentów
Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Ataki typu Deniał of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Nieautoryzowana modyfikacji odanych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne i przecwnych. Litrata danych w wyniku awarii sprzętu lub oprogramowania. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		brute force.	2.3 Modyfikacja					bezpieczeństwa.
akademickich techniczne i organizacyjne. Ataki typu Denial of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników reze nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników reze nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników prez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								
techniczne i organizacyjne. Ataki typu Deniał of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursków) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		• •					•	•
organizacyjne. Ataki typu Denial of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Nieautoryzowana modyfikacja danych osobowych studentów i przez użytkowników z uprawnieniami administracyjnymi. Atak wemnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.			akademickich				•	
Ataki typu Denial of Service (DoS) uniemožliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny- zagrożenie techniczne. Nieautoryzowana modyfikacja danych administracyjnymi. Atak wewnętrzny- zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (pp. ataki SQL injection). Atak zewnętrzny- zagrożenie techniczne i danych osobowych studentów i pracowników przez nieautoryzowane osoby (pp. ataki SQL injection). Atak zewnętrzny- zagrożenie techniczne i Organizacyjne. Wrozbania danych z uprawnieniami administracyjnymi. Atak zewnętrzny- zagrożenie techniczne i Organizacyjne. Wrozbania danych z uprawnieniami adaych osobowych studentów i pracowników przez nieautoryzowane osoby (pp. ataki SQL injection). Atak zewnętrzny- zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								
Service (DoS) uniemožliviające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny zagrożenie nodyfikacji ocen, przechwycenie danych osobowych studentów z uprawnieniami administracyjnymi. Atak wewnętrzny zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane cosoby (np. ataki SQL injection). Atak zewnętrzny zagrożenie techniczne i Utrata danych w wyniku awarii sprzętu lub oprogramowania.			wstrzyknięcie				_	Analiza i optymalizacja
uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Mieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych w wynika wawrii sprzętu lub oprogramowania.			złośliwego kodu SQL					
korzystanie z systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata krytycznych danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		1						serwerowych.
systemu w okresach wzmożonego ruchu. Atak zewnętrzny - zagrożenie techniczne. Możliwość modyfikacji ocen, przechwycenie danych osobowych studentów i pracowników. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników i pracy użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								2.2.0
Atak zewnętrzny- zagrożenie techniczne. Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny- zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny- zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		1					· · ·	~
Atak zewnętrzny - zagrożenie techniczne. Nieautoryzowana modyfikacji ocen, przechwycenie danych osobowych studentów i pracowników. z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne i organizacyjne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		1 -	danych akademickich				·	działań
zagrożenie techniczne. Możliwość modyfikacji ocen, przechwycenie danych osobowych studentów i pracowników. Atak wewnętrzny - zagrożenie danych osobowych studentów i przechwycenie danych osobowych studentów i przechwycenie danych osobowych studentów i pracowników. Atak wewnętrzny - zagrożenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		Atak zownotrzny	Skutok:					
techniczne. Nieautoryzowana modyfikacji ocen, przechwycenie danych osobowych studentów i pracowników. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		• •						
Nieautoryzowana modyfikacja danych osobowych studentów i pracowników. Przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.							,	·
Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								
modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lio oprogramowania.		Nieautoryzowana					•	
zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lu oprogramowania. kopii zapasowych. Redundancja danych. Testowanie planów odzyskiwania danych po awarii. 2.5 Regularne testy odzyskiwania danych. Monitorowanie i analiza logów aplikacji. Monitorowanie i analiza logów aplikacjinych. Testy penetracyjne. 2.5 Regularne testy odzyskiwania danych. Monitorowanie i analiza logów aplikacjinych. Testy penetracyjne. 2.5 Regularne testy odzyskiwania danych. Monitorowanie i analiza logów aplikacjinych. Testy penetracyjne. 2.5 Regularne testy odzyskiwania danych. Monitorowanie i analiza logów aplikacjinych. Testy penetracyjne.		<u> </u>					,	2.4 Regularne audyty
przez użytkowników z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		akademickich (ocen,	pracowników.				2.5 Regularne tworzenie	bezpieczeństwa
z uprawnieniami administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		zapisów kursów)					kopii zapasowych.	aplikacji.
administracyjnymi. Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		1 -						
Atak wewnętrzny - zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		•					· ·	~
zagrożenie techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.							·	
techniczne i organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								
organizacyjne. Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		•						•
Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								
danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		organizacyjne.						
studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		Przechwycenie						oprogramowania.
pracowników przez nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		1 -						Audyty kopii
nieautoryzowane osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								zapasowych.
osoby (np. ataki SQL injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		•						
injection). Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		I						
Atak zewnętrzny - zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.								
zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		injection).						
zagrożenie techniczne. Utrata danych w wyniku awarii sprzętu lub oprogramowania.		Atak zewnetrzny -						
Utrata danych w wyniku awarii sprzętu lub oprogramowania.		• •						
wyniku awarii sprzętu lub oprogramowania.								
wyniku awarii sprzętu lub oprogramowania.								
sprzętu lub oprogramowania.		<u> </u>						
oprogramowania.								
		oprogramowania.						
Zagrożenie		Zagrożenie						
techniczne.		_						

Baza danych			5	5	4		
chorych NFZ	Nieautoryzowany	3.1. Złamanie hasła:				3.1. Uwierzytelnianie	3.1. Monitorowanie
•	dostęp do danych	phishing, brute force				dwuskładnikowe.	logów dostępu.
	medycznych poprzez	, and a second				Szyfrowanie danych w	Regularne testy
	ataki phishingowe	3.2 Atak DoS:				spoczynku i w tranzycie.	penetracyjne. Audyty
	lub brute force.	przeciążenie serwera				Edukacja	bezpieczeństwa.
	iab brace forcer	przeciązenie serwera				użytkowników.	bezpieczenstwa.
	Atak zewnętrzny -	3.3 Modyfikacja				azytkowiikow.	3.2 Regularne testy
	zagrożenie	danych: fałszowanie				3.2 Ochrona DDoS od	obciążeniowe.
	techniczne i	danych medycznych				dostawców usług.	Monitorowanie
	organizacyjne.	danyen medyeznyen				Redundancja serwerów.	wydajności systemu.
	organizacyjne.	3.4 Atak SQL injection:				Monitorowanie ruchu	Analiza i optymalizacj
	Ataki typu Denial of	wstrzyknięcie				sieciowego.	zasobów
	Service (DoS)	złośliwego kodu SQL				sieciowego.	
	· · ·	ziosiiwego kodu SQL				3.3 Ścisła kontrola	serwerowych.
	uniemożliwiające	2 5 A					2.2.0
	dostęp do bazy	3.5 Awaria sprzętu:				dostępu. Audyty działań	3.3 Regularna
	danych.	utrata krytycznych				administracyjnych.	weryfikacja logów
		danych medycznych				Szyfrowanie danych w	działań
	Atak zewnętrzny -					bazie danych.	administracyjnych.
	zagrożenie						Audyty
	techniczne.	Skutek:				3.4 Regularne testy	bezpieczeństwa.
		Naruszenie poufności				penetracyjne.	Szkolenia dla
		danych medycznych				Wdrożenie WAF (Web	administratorów.
	Nieautoryzowana	pacjentów, możliwość				Application Firewall).	
	modyfikacja danych	wykorzystania danych				Edukacja	3.4 Regularne audyty
	medycznych przez	do szantażu lub				użytkowników.	bezpieczeństwa
	użytkowników z	kradzieży tożsamości.					aplikacji.
	uprawnieniami					3.5 Regularne tworzenie	Monitorowanie i
	administracyjnymi.					kopii zapasowych.	analiza logów
						Redundancja danych.	aplikacyjnych. Testy
	Atak wewnętrzny -					Testowanie planów	penetracyjne.
	zagrożenie					odzyskiwania danych po	
	techniczne i					awarii.	3.5 Regularne testy
	organizacyjne.						odzyskiwania danych.
							Monitorowanie stanu
							sprzętu i
	Przechwycenie						oprogramowania.
	danych medycznych						Audyty kopii
	przez						zapasowych.
	nieautoryzowane						
	osoby (np. ataki SQL						
	injection).						
	Atak zewnętrzny -						
	zagrożenie						
	techniczne.						
	Utrata danych w						
	wyniku awarii						
	sprzętu lub						
	onrogramowania	1	İ	1	1	1	İ

oprogramowania.

Zagrożenie techniczne.

Managarlia			4	2	2		
Kamerka	Nicautomacus	4.1 Infokcia makwara:	4	3	2	4.1 H i wwania	4.1 Pogularno
komputerowa	Nieautoryzowany	4.1 Infekcja malware:				4.1 Używanie	4.1 Regularne
	dostęp do kamerki	zdalne przejęcie				oprogramowania 	skanowanie systemu
	internetowej przez	kontroli nad kamerką				antywirusowego.	pod kątem malware.
	złośliwe	4 2 4 1 4 4 7 4				Regularne aktualizacje	Monitorowanie logów
	oprogramowanie	4.2 Atak MITM:				systemu i sterowników.	dostępu do kamerki.
	(malware).	przechwycenie obrazu				Uwierzytelnianie	Testy penetracyjne.
						dwuskładnikowe.	
	Atak zewnętrzny -	4.3 Modyfikacja					4.2 Regularne audyty
	zagrożenie	ustawień: zmiana				4.2 Włączenie	bezpieczeństwa. Testy
	techniczne.	konfiguracji				szyfrowania	bezpieczeństwa
		urządzenia				komunikacji. Używanie	komunikacji.
	Podszywanie się pod					bezpiecznych sieci.	Monitorowanie logów.
	urządzenie i	4.4 Awaria sprzętu:				Regularne aktualizacje	
	przechwycenie	niemożność				oprogramowania.	4.3 Regularne audyty
	obrazu (np. ataki	korzystania z					ustawień urządzenia.
	typu Man-in-the-	urządzenia				4.3 Uwierzytelnianie	Monitorowanie logów
	Middle).					dwuskładnikowe.	zmian ustawień. Testy
		Skutek:				Szyfrowanie ustawień	penetracyjne.
	Atak wewnętrzny –	Naruszenie				urządzenia. Regularne	
	zagrożenie	prywatności				aktualizacje firmware'u.	4.4 Regularne testy
	techniczne.	użytkownika,					urządzenia.
		możliwość szantażu,				4.4 Regularne testy	Monitorowanie stanu
	Nieautoryzowana	przechwycenie				funkcjonalności.	sprzętu. Audyty
	modyfikacja	poufnych informacji.				Aktualizacje	aktualności
	ustawień kamerki					oprogramowania. Kopie	oprogramowania.
	przez atakującego.					zapasowe ustawień.	
	Atak wewnętrzny –						
	zagrożenie						
	techniczne.						
	Utrata dostępu do						
	kamerki w wyniku						
	awarii sprzętu lub						
	oprogramowania.						
	Zagrożenie						
	techniczne.						

Baza danych			5	5	3		
odcisków	Nieautoryzowany	5.1. Złamanie hasła:			_	5.1. Uwierzytelnianie	5.1. Monitorowanie
palców	dostęp do danych	phishing, brute force				dwuskładnikowe.	logów dostępu.
•	biometrycznych	, o,				Szyfrowanie danych w	Regularne testy
	przez ataki	5.2 Atak DoS:				spoczynku i w tranzycie.	penetracyjne. Audyty
	phishingowe lub	przeciążenie serwera				Edukacja	bezpieczeństwa.
	brute force.					użytkowników.	•
		5.3 Modyfikacja				,	5.2 Regularne testy
	Atak zewnętrzny -	danych: fałszowanie				5.2 Ochrona DDoS od	obciążeniowe.
	zagrożenie	danych				dostawców usług.	Monitorowanie
	techniczne i	biometrycznych				Redundancja serwerów.	wydajności systemu.
	organizacyjne.					Monitorowanie ruchu	Analiza i optymalizacja
		5.4 Atak SQL injection:				sieciowego.	zasobów
	Ataki typu Denial of	wstrzyknięcie					serwerowych.
	Service (DoS)	złośliwego kodu SQL				5.3 Ścisła kontrola	
	uniemożliwiające					dostępu. Audyty działań	5.3 Regularna
	dostęp do bazy	5.5 Awaria sprzętu:				administracyjnych.	weryfikacja logów
	danych.	utrata krytycznych				Szyfrowanie danych w	działań
		danych				bazie danych.	administracyjnych.
	Atak zewnętrzny -	biometrycznych					Audyty
	zagrożenie					5.4 Regularne testy	bezpieczeństwa.
	techniczne.	Skutek:				penetracyjne.	Szkolenia dla
		Naruszenie poufności				Wdrożenie WAF (Web	administratorów.
		danych				Application Firewall).	
	Nieautoryzowana	biometrycznych,				Edukacja	5.4 Regularne audyty
	modyfikacja danych	możliwość				użytkowników.	bezpieczeństwa
	biometrycznych	wykorzystania danych				E E Danislama Assaula	aplikacji.
	przez użytkowników	do kradzieży				5.5 Regularne tworzenie	Monitorowanie i
	z uprawnieniami	tożsamości.				kopii zapasowych. Redundancja danych.	analiza logów
	administracyjnymi.					Testowanie planów	aplikacyjnych. Testy
	Atak wewnętrzny -					odzyskiwania danych po	penetracyjne.
	zagrożenie					awarii.	5.5 Regularne testy
	techniczne i					awaiii.	odzyskiwania danych.
	organizacyjne.						Monitorowanie stanu
	organizacyjne.						sprzętu i
	Przechwycenie						oprogramowania.
	danych						Audyty kopii
	biometrycznych						zapasowych.
	przez						, ,
	nieautoryzowane						
	osoby (np. ataki SQL						
	injection).						
	Atak zewnętrzny -						
	zagrożenie						
	techniczne.						
	Utrata danych w						
	wyniku awarii						
	sprzętu lub						
	oprogramowania.						
	Zagrożenie						
	techniczne.						
			1	1	l		1