ЖҮЙЕНІ ҚОРҒАУ ЖӘНЕ ҚАУІПСІЗДІК

Шахмуханбетов Ханкелді

Нариман Бағыбек

Еренгалиев Айсын

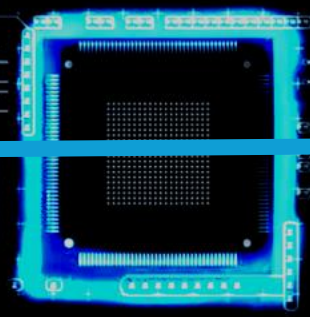
Шахмуханбетов Нұргелді

Болат Арна

КІРІСПЕ

Ақпараттық жүйелердің қауіпсіздігі мен қорғалуын қамтамасыз ету қазіргі заманғы технологияның маңызды аспектісі болып табылады. Қауіпсіздік және деректерді қорғау ұғымдары арасындағы айырмашылық қауіпсіздік жүйелерін әзірлеу және енгізу кезінде өте маңызды. Терминдердің дифференциациялануы ақпараттық қауіпсіздік саласындағы мақсаттар мен міндеттерді неғұрлым нақты анықтауға мүмкіндік береді.

ҚАУІП СІЗДІК МІНДЕТ ТЕРІ МЕН ҚАУІПТЕРІ



Құпиялылық

Қол жетімділік

Тұтастық

Құпиялылық

Мәліметтерді қорғаудың негізгі міндеттерінің бірі ақпараттың құпиялылығын қамтамасыз ету, яғни рұқсат етілмеген қол жеткізуден қорғау болып табылады.

Деректерді қорғау

Құпиялылық деректерді рұқсатсыз кіруден қорғауға бағытталған, өйткені құпия ақпаратты ашу ауыр зардаптарға әкелуі мүмкін.

Рұқсат құқығы

Деректерге қол жеткізу құқықтарын анықтау қажеттілігі ақпараттың құпиялылығын қамтамасыз етуге және ағып кетудің алдын алуға көмектеседі.

Қол жетімділік

Қол жетімділік

Деректер қажет кезде қолжетімді болатынына сенімділік те маңызды.

Қолжетімділігін анықтау

Деректерге тұрақты қол жеткізуді қамтамасыз ету жүйенің біркелкі жұмыс істеуі және пайдаланушы тәжірибесі үшін маңызды.

Қолжетімділік шабуылдары

Деректердің қолжетімділігіне бағытталған шабуылдардың әртүрлі түрлері мұқият бақылау мен қорғауды қажет етеді.

түрлері мұқият бақылау мен қорғауды қажет етеді.

Тұтастық

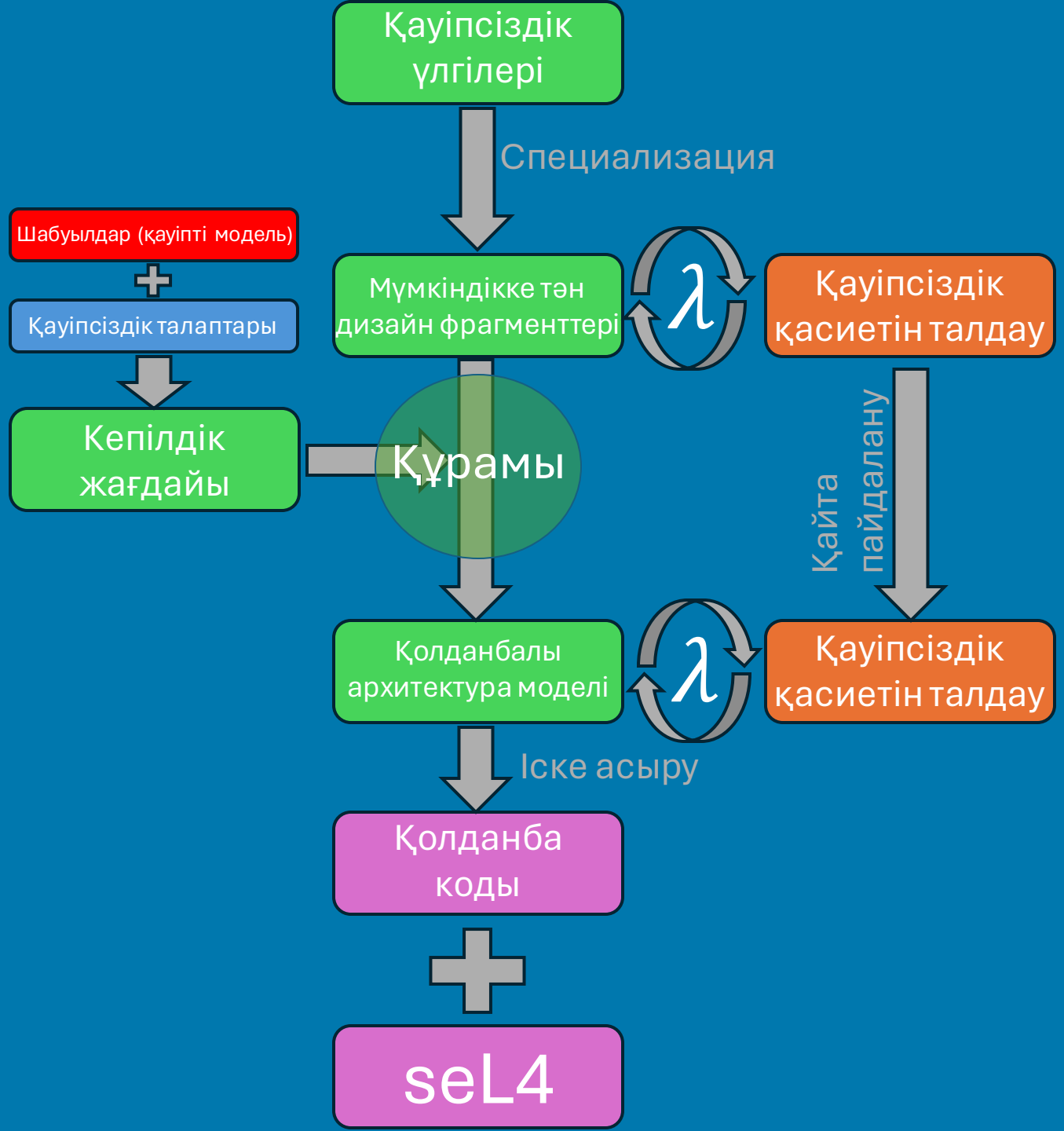
Маңызды міндет - рұқсатсыз өзгертуге болмайтындай деректердің тұтастығына кепілдік беру.

Бұзушылықтан қорғау

Тұтастық деректерді қажетсіз өзгерістерден қорғауға, оның тұтастығын қамтамасыз етуге бағытталған.

Өзгерістердің түрлері

Деректерді өзгертудің әртүрлі түрлері қолайсыз салдарға әкелуі мүмкін, сондықтан олардың алдын алу маңызды.


Қауіпсіздік үлгілері
Специализация
Шабуылдар (қауіпті модель)
Қауіпсіздік талаптары
Мүмкіндікке тән дизайн фрагменттері
λ
Қауіпсіздік қасиетін талдау
Кепілдік жағдайы
Құрамы
Қайта пайдалану
Қолданбалы архитектура моделі
λ
Қауіпсіздік қасиетін талдау
Іске асыру
Қолданба коды
seL4

БҰЗУШЫЛЫҚ ҚҰРАЛДАРЫ

Nmap

nmap – желі құрылғыларындағы осалдықтарды анықтай алатын желіні сканерлеу және қауіпсіздік аудитін автоматтандырудың қуатты құралы.

Dsniff

dsniff - желілік трафикті тыңдауға, құпия сөздерді ұстап алуға және шифрланған ақпаратты талдауға арналған құралдар жиынтығы.

LOIC

LOIC (Low Orbit Ion Cannon) – DDoS шабуылдарын жүзеге асыру және мақсатты серверлерге зақым келтіру үшін пайдаланылатын ашық бастапқы бағдарламалық құрал.

Metasploit

Metasploit - бұл эксплойттерді әзірлеу және пайдалану мүмкіндігі бар осалдықты тексеру және қауіпсіздікті тексеру платформасы.

БОТНЕТТЕР ЖӘНЕ ОЛАРДЫҢ САЛДАРЫ

1
Инфекция

Вирус жұққан компьютер

2
Байланыс

Команда және басқару орталығы (C2)

Хакер
(Botmaster)

Зиянды бағдарламаны тарату

Спам email

Вирус жұққан веб-сайттар

Әлеуметтік желідегі жазбалар

Botnet

3
Бақылау

4
Көбейту

ботнеттік киберқылмыс

Киберқылмыс қаупі

Ботнеттер киберқылмыста әртүрлі нысандарға қарсы ауқымды шабуылдар үшін қолданылады.

КИБЕРШАБУЫЛДАРДАН ҚОРҒАУ БОЙЫНША ҰСЫНЫСТАР

Қорғау шараларына шолу

Қазіргі ақпараттық әлемде кибершабуылдардан қорғау маңызды рөл атқарады. Ұйымдар мен жеке тұлғалар өздерінің деректері мен жүйелерінің әртүрлі қауіптерден қорғалуын қамтамасыз етуі керек. Бұған көп деңгейлі аутентификация, деректерді шифрлау, желі брандмауэрін пайдалану және бағдарламалық құралды тұрақты жаңарту сияқты шаралар кіруі мүмкін. Сонымен қатар, мониторинг және оқиғаларды анықтау жүйелерін (SIEM) енгізу ақпараттық жүйе қауіпсіздігінің маңызды құрамдас бөлігі болып табылады.

Проактивті әрекеттер

Қауіпсіздікті басқару элементтерін орнатумен қатар, осалдықтарды анықтауда және ықтимал қауіптерге жауап беруде белсенділік таныту маңызды. Бұған қауіпсіздік жүйелерінің тұрақты аудитін жүргізу, қызметкерлерді киберқауіпсіздік негіздеріне үйрету, желілік трафикті бақылау және талдау үшін бағдарламаларды орнату кіреді. Алдын ала шаралар кибершабуыл қаупін айтарлықтай төмендетіп, жалпы қауіпсіздікті жақсартады.

ҚОРЫТЫНДЫЛАР МЕН ҰСЫНЫТАР

Ақпараттық жүйе қауіпсіздігінің негізгі түсініктерін және олармен байланысты қауіптерді зерттегеннен кейін тиімді қорғау үшін бірнеше ұсыныстар ұсына аламыз. Біріншіден, бағдарламалық құралды жаңартып отыру керек және жүйелерге кіру үшін күшті құпия сөздерді пайдалану керек. Сондай-ақ тұрақты қауіпсіздік аудитін жүргізу және қызметкерлерді құпия ақпаратпен жұмыс істеуге үйрету маңызды.

Рұқсат етілмеген кіруден қорғау үшін деректерді шифрлауды және көп деңгейлі аутентификацияны пайдалану маңызды. Сонымен қатар, кенеттен кибершабуыл болған жағдайда деректердің сақтық көшірмесін жасау маңызды. Жалпы алғанда, тиімді қорғау технологиялық, технологиялық және оқыту шараларын қамтитын кешенді тәсілге негізделген.