ДӘРІС 5

Кибершабуылдарды анықтауда жасанды интеллект пен машиналық оқытуды қолдану

Оқытушы: проф. Ахмедиярова А.Т.

Негізгі ұғымдар

Негізгі ұғымдар

Бақыланатын оқыту — Белгіленген деректерден класс үйренетін тәсіл. Бақыланбайтын оқыту — Класс белгісінсіз құрылым мен ауытқуды іздеу. Терең оқыту — Көпқабатты нейрондық желілер арқылы күрделі заңдылықтарды үйрену. Гибридті тәсіл — Ереже мен ML әдістерін біріктіру.

Бақыланатын оқыту

Қалыпты/шабуыл мысалдары қажет. Белгілі кластарды жақсы ажыратады. Сонымен бірге сапалы белгіленген деректер қажет. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Бақыланбайтын оқыту

Кластерлер мен аномалияларды анықтайды. Белгісіз шабуылдарды іздеуге қолайлы. Сонымен бірге нәтижені интерпретациялау күрделірек. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Терең оқыту

Терең оқыту

Үлкен және күрделі деректерге бағытталған. Күрделі тәуелділіктерді үйрене алады. Сонымен бірге есептеу ресурсы мен дерек көлемін қажет етеді. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Гибридті тәсіл

Белгілі және белгісіз қауіптерді бірге талдайды. Қамтуды арттырады. Сонымен бірге архитектурасы күрделі. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Қорғаныстық қолдану

Қарастырылған әдістер жеке-жеке емес, көпдеңгейлі киберқорғаныс құрамында тиімді. Деректерді жинау, қалыпқа келтіру, талдау, қауіп деңгейін бағалау және әрекет ету біртұтас процесс ретінде ұйымдастырылады. Интеллектуалды компоненттер үлкен көлемдегі оқиғаларды өңдеуге көмектеседі, ал соңғы шешім тәуекел мен контекстті ескере отырып қабылданады.

Қорытынды

Қорытынды

Кибершабуылдарды анықтауда жасанды интеллект пен машиналық оқытуды қолдану кибершабуылдарды анықтау және оларға қарсы әрекет ету жүйесінің маңызды бөлігі болып табылады. Тиімділік бір ғана құралға емес, әдістерді дұрыс біріктіруге, деректер сапасына, тұрақты мониторингке және нәтижелерді тексеруге тәуелді.

Бақылау сұрақтары

1. Негізгі ұғымдарға анықтама беріңіз. 2. Кестеде берілген тәсілдердің негізгі айырмашылықтары қандай? 3. Әр тәсілдің артықшылығы неде? 4. Негізгі кемшіліктері қандай? 5. Қандай деректер талданады? 6. Қандай жағдайда гибридті тәсіл тиімді? 7. Жалған оң және жалған теріс нәтиженің әсері қандай? 8. Интеллектуалды әдістердің рөлі қандай? 9. Қарастырылған схема кезеңдерін түсіндіріңіз. 10.

Бақылау сұрақтары

Бұл тәсіл кешенді киберқорғаныспен қалай байланысады?

Список источников

Список источников

1. Менщиков А.А., Заколдаев Д.А., Воробьева А.А. Введение в кибербезопасность и киберустойчивость: учебно-методическое пособие. — Санкт-Петербург: Университет ИТМО, 2024. — 72 с. 2. Вострецова Е.В. Основы информационной безопасности: учебное пособие. — Екатеринбург: Издательство Уральского университета, 2019. — 204 с. — ISBN 978-5-7996-2677-8. 3. Назарян А.К., Карцан И.Н.

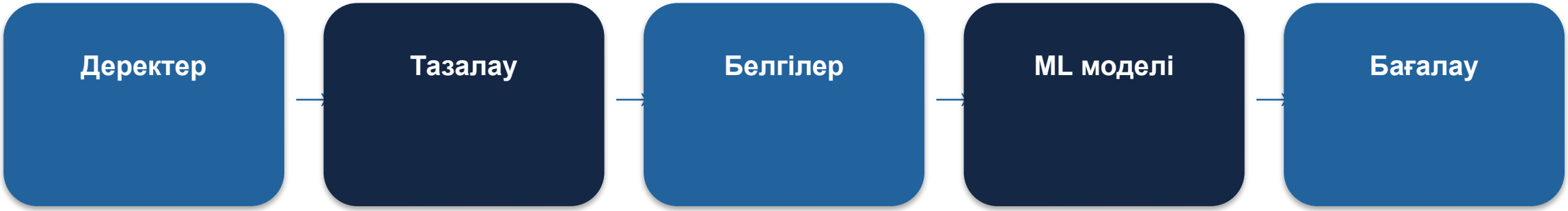
Список источников

Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. — 2025. — Т. 4, № 1. — С. 1001–1007.

Негізгі әдістер мен сипаттамаларды салыстыру

Түрі/тәсілі	Анықтамасы	Ерекшелігі	Артықшылығы	Кемшілігі
Бақыланатын оқыту	Белгіленген деректерден класс үйренетін тәсіл.	Қалыпты/шабуыл мысалдары қажет.	Белгілі кластарды жақсы ажыратады.	Сапалы белгіленген деректер қажет.
Бақыланбайтын оқыту	Класс белгісінсіз құрылым мен ауытқуды іздеу.	Кластерлер мен аномалияларды анықтайды.	Белгісіз шабуылдарды іздеуге қолайлы.	Нәтижені интерпретациялау күрделірек.
Терең оқыту	Көпқабатты нейрондық желілер арқылы күрделі заңдылықтарды үйрену.	Үлкен және күрделі деректерге бағытталған.	Күрделі тәуелділіктерді үйрене алады.	Есептеу ресурсы мен дерек көлемін қажет етеді.
Гибридті тәсіл	Ереже мен ML әдістерін біріктіру.	Белгілі және белгісіз қауіптерді бірге талдайды.	Қамтуды арттырады.	Архитектурасы күрделі.

Жүйенің жалпы жұмыс істеу архитектурасы



Әр кезеңнің нәтижесі келесі кезеңнің кіріс дерегі болады. Мониторинг пен тексеру нәтижелері қорғаныс шешімін нақтылауға мүмкіндік береді.

Түйінді ұғымдар және қолданылуы

Негізгі ұғымдар

Бақыланатын оқыту — Белгіленген деректерден класс үйренетін тәсіл. Бақыланбайтын оқыту — Класс белгісінсіз құрылым мен ауытқуды іздеу. Терең оқыту — Көпқабатты нейрондық желілер арқылы күрделі заңдылықтарды үйрену. Гибридті тәсіл — Ереже мен ML әдістерін біріктіру.

Бақыланатын оқыту

Қалыпты/шабуыл мысалдары қажет. Белгілі кластарды жақсы ажыратады. Сонымен бірге сапалы белгіленген деректер қажет. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Бақыланбайтын оқыту

Кластерлер мен аномалияларды анықтайды. Белгісіз шабуылдарды іздеуге қолайлы. Сонымен бірге нәтижені интерпретациялау күрделірек. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Терең оқыту

Үлкен және күрделі деректерге бағытталған. Күрделі тәуелділіктерді үйрене алады. Сонымен бірге есептеу ресурсы мен дерек көлемін қажет етеді. Сондықтан бұл тәсілді нақты ақпараттық жүйенің архитектурасы, қауіп моделі, деректер сапасы және қолданыстағы қорғаныс механизмдерімен бірге қарастыру қажет.

Қорытынды және талдау сұрақтары

Негізгі қорытынды

Кибершабуылдарды анықтауда жасанды интеллект пен машиналық оқытуды қолдану. Қорғаныс шешімін қабылдағанда деректер сапасы, жүйенің контексті және тәуекел деңгейі бірге бағаланады.

Талдау тапсырмасы

Берілген жүйе үшін негізгі активтерді, қауіп белгілерін, анықтау әдісін және қорғаныс шараларын бір сызбада көрсетіңіз.

Салыстыру

Қарастырылған тәсілдердің артықшылықтары мен шектеулерін нақты мысал арқылы түсіндіріңіз.