ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
МАҚАН ЕСБОЛАТОВ атындағы АЛМАТЫ АКАДЕМИЯСЫ

ИНТЕРНЕТТЕГІ АЛАЯҚТЫҚТЫ АНЫҚТАУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТТІ ПАЙДАЛАНУ

дөңгелек үстел материалдары
20 қыркүйек 2024 ж

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ВЫЯВЛЕНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВ

материалы круглого стола
20 сентября 2024 г

Алматы, 2024

УДК 004.8
ББК 32.813
И88

И88 Интернеттегі алаяқтықты анықтау үшін жасанды интеллектті пайдалану: дөңгелек үстел материалдары (20.09.2024ж.) = Использование возможностей искусственного интеллекта для выявления интернет-мошенничеств: материалы круглого стола (20.09.2024г.) – Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан им. М. Есбулатова, 2024. – 78 с.

ISBN 978-601-360-158-8

Жинақта «Интернеттегі алаяқтықты анықтау үшін жасанды интеллектті пайдалану» дөңгелек үстелі қатысушыларының ғылыми баяндамалары ұсынылған. Дөңгелек үстелі жинағы құқық қорғау органдары жоғары оқу орындарының, басқа да заң жоғары оқу орындарының оқытушыларына, докторанттары мен магистранттарына, ішкі істер органдарының тәжірибелік қызметкерлеріне, сондай-ақ қалың көлемдегі оқырмандарға арналған.

В сборнике представлены научные доклады участников заочного круглого стола «Использование возможностей искусственного интеллекта для выявления интернет-мошенничеств». Сборник круглого стола рассчитан на преподавателей, докторантов и магистрантов высших учебных заведений правоохранительных органов, других юридических вузов, практических работников органов внутренних дел, а также широкому кругу читателей.

Жинақтағы материалдар автордың редакциясымен берілді.
Материалы, публикуемые в сборнике, даны в авторской редакции.

УДК 004.8
ББК 32.813

ISBN 978-601-360-158-8

«Интернеттегі алаяқтықты анықтау үшін жасанды интеллект мүмкіндіктерін пайдалану» тақырыбындағы дөңгелек үстел бағдарламасы		
Өткізу күні:	*20 қыркүйек 2024 жыл*. (басталу уақыты Астана уақытымен сағат 10:00)	
Өткізу орны:	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасы	
Өткізу форматы:	offline / online аралас формат-ZOOM байланыс платформасын қолдана отырып	
11:00 – 11:30	**Кадырова Рашида Турсыновна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасы бастығы полиция подполковнигі	Приветственное слово
	Шоханов Азамат Канатович Қазақстан Республикасы ІІМ Криминалдық полиция департаментінің киберқылмыспен күресу орталығының аса маңызды істер бойынша аға жедел уәкілі полиция капитаны	Использование потенциала искусственного интеллекта для обнаружения интернет-мошенничества в Республике Казахстан
11:30 - 11:40	**Лемайкина Светлана Владимировна** Федералдық мемлекеттік қазынашылық жоғары оқу орны Ресей Федерациясы ІІМ Ростов заң институтының ІІО ақпараттық қамтамасыз ету кафедрасының аға оқытушысы	Общий искусственный интеллект в правоохранительных органах
11:40 - 11:50	**Кебекпаев Жасулан Серикович** «MSSP Global» компаниясының техникалық директоры	Киберугрозы: основные виды, последствия и методы защиты
11:50 – 12:00	**Дурсунов Руслан Ниязович** Ақпараттық қауіпсіздік бойынша эксперт	Информационная безопасность в республике казахстан: вызовы и решения
12:00 – 12: 10	**Мағазов Райымбек Саламатұлы** Әл-Фараби атындағы КазҰУ-нің докторанты	Дипфейки: технология, риски и способы противодействия
12:10 – 12:20	**Алимжанова Жанна Муратбековна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының профессоры, ф-м.ғ.к.	Инструменты и методы обнаружения дипфейков
12:20 – 12:30	**Айтбаева Рахатай Бекбергеновна** Алматы технологиялық университеті, «Ақпараттық жүйелер» кафедрасының лекторы	Применение искусственного интеллекта для выявления интернет-мошенничества
12:30 – 12:40	**Тасбулатов Руслан Ермекович** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнына кейінгі білім беру факультетінің 2 курс магистранты полиция капитаны	Технология исскуственного интеллекта в раскрытии и изобличении интернет преступлений
12:40 – 12:50	**Бейсенбі Арна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнына кейінгі білім беру факультетінің 2 курс магистранты полиция аға лейтенанты	Кибербуллинг : онлайн қорқыту және қорлау үшін жауапкершілік мәселелері

12:50 – 13:00	**Смайлов Нұржігіт Куралбаевич** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының профессоры, PhD	Основные методы и подходы для распознавания речи с целью защиты от интернет-мошенничества
13:00 – 13:10	**Кубанова Нургуль Байтоковна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнына кейінгі білім беру факультетінің 3 курс докторанты полиция майоры	Ddos шабуылдары және интернеттегі алаяқтық: қауіптер мен қорғаныс шаралары
13:10 – 13:20	**Белгожаева Лаззат Серикбаевна** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының аға оқытушысы полиция подполковнигі	Интернеттегі алаяқтықты анықтаудағы жасанды интеллекттің мүмкіндігі
13:20 – 13:30	**Қуаныш Дәурен Қалижанұлы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасы бастығының орынбасары полиция капитаны	Применение технологий искусственного интеллекта для обнаружения интернет-мошенничеств
13:30 – 13:40	**Ендыбайұлы Ерлан** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының доценті полиция майоры	Обнаружение фальшивых учетных записей и спам-аккаунтов: современные методы и технологии
13:40 – 13:50	**Савдабаев Ержан Сәрсенович** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы полиция аға лейтенанты	Инструменты ии для распознавания синтезированных голосов и поддельных документов
13:50 – 14:00	**Сәбиболда Әкежан Мұратұлы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы полиция лейтенанты	Биометрическая аутентификация по голосу: технологии, преимущества
14:00 – 14:10	**Уралова Фатима Сырлыбайқызы** Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы, полиция лейтенанты	Применение искусственного интеллекта в выявлении фальшивых аккаунтов в социальных сетях
14:10 – 14:20	**Рамазанова Жаннұр Ерқалықызы** Satbayev University 2 курс магистранты	Разработка защищенной системы аутентификации для информационной системы вуза
14:20 – 14:40	Пікірталас	
14:45 – 14:55	Қорытындылау, қарарды талқылау	
14:55 – 15:00	Дөңгелек үстелді аяқтау	

Программа круглого стола на тему «Использование возможностей искусственного интелекта для выявления интернет-мошеничеств»		
Дата проведения:	*20 сентября 2024 года.* *(время начала в 10: 00 по времени Астаны)*	
Место проведения:	Кафедра кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова	
Формат проведения:	Смешанный формат offline / online-с использованием коммуникационной платформы ZOOM	
Модератор:	**Кадырова Рашида Турсуновна** Начальник кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова, ассоциированный профессор, полковник полиции	
11:00 – 11:30	**Кадырова Рашида Турсыновна** Начальник кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова, ассоциированный профессор, подполковник полиции	Приветственное слово
	Шоханов Азамат Канатович Старший оперуполнмоченный по особо важным делам Центра по борьбе с киберпреступностью Департамента криминальной полиции МВД Республики Казахстан капитан полиции	Использование потенциала искусственного интеллекта для обнаружения интернет-мошенничества в Республике Казахстан
11:30 - 11:40	**Лемайкина Светлана Владимировна** Старший преподаватель кафедры информационного обеспечения ОВД Ростовского юридического института МВД России	Общий искусственный интеллект в правоохранительных органах
11:40 - 11:50	**Кебекпаев Жасулан Серикович** Технический директор компании «MSSP Global»	Киберугрозы: основные виды, последствия и методы защиты
11:50 – 12:00	**Дурсунов Руслан Ниязович** Эксперт по Информационной безопасности	Информационная безопасность в республике казахстан: вызовы и решения
12:00 – 12: 10	**Магазов Райымбек Саламатулы** Докторант 1 курса КазНУ имени Аль-Фараби	Дипфейки: технология, риски и способы противодействия
12:10 – 12:20	**Алимжанова Жанна Муратбековна** Профессор кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ф-м.н.	Инструменты и методы обнаружения дипфейков
12:20 – 12:30	**Айтбаева Рахатай Бекбергеновна** Лектор кафедры «Информационные системы» Алматинского технологического университета	Применение искусственного интеллекта для выявления интернет-мошенничества
12:30 – 12:40	**Тасбулатов Руслан Ермекович** Магистрант 2 курса факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции	Технология исскуственного интеллекта в раскрытии и изобличении интернет преступлений

12:40 – 12:50	**Бейсенбі Арна** Магистрант 2 курса факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова старший лейтенант полиции	Кибербуллинг : онлайн қорқыту және қорлау үшін жауапкершілік мәселелері
12:50 – 13:00	**Смайлов Нуржигит Куралбаевич** Профессор кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова, PhD	Основные методы и подходы для распознавания речи с целью защиты от интернет-мошенничества
13:00 – 13:10	**Куаныш Даурен Калижанулы** Заместитель начальника кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции	Ddos шабуылдары және интернеттегі алаяқтық: қауіптер мен қорғаныс шаралары
13:10 – 13:20	**Кубанова Нургуль Байтоковна** Докторант 3 курса факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции	Интернеттегі алаяқтықты анықтаудағы жасанды интеллекттің мүмкіндігі
13:20 – 13:30	**Белгожаева Лаззат Серикбаевна** Старший преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции	Применение технологий искусственного интеллекта для обнаружения интернет-мошенничеств
13:30 – 13:40	**Ендыбайұлы Ерлан** Доцент кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции	Обнаружение фальшивых учетных записей и спам-аккаунтов: современные методы и технологии
13:40 – 13:50	**Савдабаев Ержан Сарсенович** Преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова старший лейтенант полиции	Инструменты ии для распознавания синтезированных голосов и поддельных документов
13:50 – 14:00	**Сабиболда Акежан Муратулы** Преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова лейтенант полиции	Биометрическая аутентификация по голосу: технологии, преимущества
14:00 – 14:10	**Уралова Фатима Сырлыбайкизи** Преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова лейтенант полиции	Применение искусственного интеллекта в выявлении фальшивых аккаунтов в социальных сетях
14:10 – 14:20	**Рамазанова Жаннұр Ерқалиқызы** Магистрант 2 курса Satbayev University	Разработка защищенной системы аутентификации для информационной системы вуза
14:20-14:40	Дискуссия	
14:40-14:55	Подведение итогов, обсуждение резолюции	
14:55-15:00	Завершение работы круглого стола	

«Интернеттегі алаяқтықты анықтау үшін жасанды интеллект мүмкіндіктерін пайдалану» атты дөңгелек үстелдің қатысушылар
ТІЗІМІ

№	Т.А.Ә.	Лауазымы
1	КАДЫРОВА Рашида Турсуновна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасы бастығы полиция подполковнигі
2	ШОХАНОВ Азамат Канатович	Қазақстан Республикасы ІІМ Криминалдық полиция департаментінің Киберқылмыспен күресу орталығының аса маңызды істер бойынша аға жедел уәкілі полиция капитаны
3	ЛЕМАЙКИНА Светлана Владимировна	Федералдық мемлекеттік қазынашылық жоғары оқу орны Ресей Федерациясы ІІМ Ростов заң институтының ІІО ақпараттық қамтамасыз ету кафедрасының аға оқытушысы
4	КЕБЕКПАЕВ Жасулан Серикович	«MSSP Global» компаниясының техникалық директоры
5	ДУРСУНОВ Руслан Ниязович	Ақпараттық қауіпсіздік бойынша эксперт
6	МАҒАЗОВ Райымбек Саламатұлы	Әл-Фараби атындағы Казақ Ұлттық Университетінің докторанты
7	АЛИМЖАНОВА Жанна Муратбековна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының профессоры, ф-м.ғ.к.
9	АЙТБАЕВА Рахатай Бекбергеновна	Алматы технологиялық университеті, «Ақпараттық жүйелер» кафедрасының лекторы
10	ТАСБУЛАТОВ Руслан Ермекович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнына кейінгі білім беру факультетінің 2 курс магистранты полиция капитаны
11	БЕЙСЕНБІ Арна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнына кейінгі білім беру факультетінің 2 курс магистранты полиция аға лейтенанты
11	СМАЙЛОВ Нұржігіт Куралбаевич	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының профессоры, PhD
12	КУБАНОВА Нургуль Байтоковна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының жоғары оқу орнына кейінгі білім беру факультетінің 3 курс докторанты полиция майоры
13	БЕЛГОЖАЕВА Лаззат Серикбаевна	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының аға оқытушысы полиция подполковнигі
14	ҚУАНЫШ Дәурен Қалижанұлы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасы бастығының

		орынбасары полиция капитаны
15	ЕНДЫБАЙҰЛЫ Ерлан	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының доценті полиция майоры
16	САВДАБАЕВ Ержан Сәрсенович	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы полиция аға лейтенанты
17	СӘБИБОЛДА Әкежан Мұратұлы	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы полиция лейтенанты
18	УРАЛОВА Фатима Сырлыбайкизи	Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының Киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы полиция лейтенанты
19	РАМАЗАНОВА Жаннұр Ерқалиқызы	Satbayev University 2 курс магистранты

СПИСОК
участников круглого стола «Использование возможностей искусственного интелекта для выявления интернет-мошеничеств»

№	Ф.И.О.	Должность
1	КАДЫРОВА Рашида Турсуновна	Начальник кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова, ассоци-ированный профессор, подполковник полиции
2	ШОХАНОВ Азамат Канатович	Старший оперуполнмоченный по особо важным делам Центра по борьбе с киберпреступностью Департамента криминальной полиции МВД Республики Казахстан капитан полиции
3	ЛЕМАЙКИНА Светлана Владимировна	Старший преподаватель кафедры информационного обеспечения ОВД, ФГКОУ ВО «Ростовский юридический институт МВД Российской Федерации»
4	КЕБЕКПАЕВ Жасулан Серикович	Технический директор компании «MSSP Global»
5	ДУРСУНОВ Руслан Ниязович	Эксперт по Информационной безопасности
6	МАГАЗОВ Райымбек Саламатулы	Докторант 1 курса КазНУ имени Аль-Фараби
7	АЛИМЖАНОВА Жанна Муратбековна	Профессор кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ф-м.н.
8	АЙТБАЕВА Рахатай Бекбергеновна	Лектор кафедры «Информационные системы» Алматинского технологического университета
9	ТАСБУЛАТОВ Руслан Ермекович	Магистрант 2 курса факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции
10	БЕЙСЕНБІ Арна	Магистрант 2 курса факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова старший лейтенант полиции
11	СМАЙЛОВ Нуржигит Куралбаевич	Профессор кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова, PhD
12	КУАНЫШ Даурен Калижанулы	Заместитель начальника кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции
13	КУБАНОВА Нургуль Байтоковна	Докторант 3 курса факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции
14	БЕЛГОЖАЕВА Лаззат Серикбаевна	Старший преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова подполковник полиции
15	ЕНДЫБАЙҰЛЫ Ерлан	Доцент кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции

16	САВДАБАЕВ Ержан Сарсенович	Преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова старший лейтенант полиции
17	САБИБОЛДА Акежан Муратулы	Преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова лейтенант полиции
18	УРАЛОВА Фатима Сырлыбайкизи	Преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова лейтенант полиции
19	РАМАЗАНОВА Жаннұр Ерқалиқызы	Магистрант 2 курса Satbayev University

КАДЫРОВА Рашида Турсыновна
начальник кафедры кибербезопасности и информационных технологий
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова подполковник полиции

ПРИВЕТСТВЕННОЕ СЛОВО

Уважаемые коллеги, дорогие друзья!

Сегодняшняя тема посвящена одной из самых актуальных проблем нашего времени – **выявлению интернет-мошенничеств с использованием возможностей искусственного интеллекта**. В век цифровой экономики и глобальной взаимосвязанности интернет стал не только удобным инструментом для общения и бизнеса, но и ареной для различных видов мошенничества. Злоумышленники используют сложные технологии для совершения киберпреступлений, и традиционные методы защиты уже не всегда эффективны.

Именно здесь на помощь приходят **технологии искусственного интеллекта**. AI способен анализировать огромные массивы данных, выявлять скрытые закономерности и прогнозировать потенциальные угрозы. Эти решения помогают нам не только быстро реагировать на атаки, но и предвидеть их, минимизируя риски для пользователей и компаний.

Мы будем обсуждать, как искусственный интеллект способен кардинально изменить подходы к борьбе с интернет-мошенничеством, какие уже существуют эффективные инструменты и как нам подготовиться к будущим вызовам. Уверена, что наше взаимодействие и обмен знаниями помогут нам лучше понять эту сложную тему и разработать стратегии, которые повысят нашу безопасность в цифровом мире.

Приятного и продуктивного обсуждения!

КУАНЫШ Даурен Калижанулы
заместитель начальника кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВ

В современном мире, где цифровизация охватывает все сферы жизни, интернет-мошенничество становится одной из самых значительных угроз как для обычных пользователей, так и для бизнеса. В последние годы масштабы киберпреступлений значительно возросли, и традиционные методы защиты, такие как антивирусные программы и системы мониторинга трафика, уже не всегда справляются с новой волной кибератак. В условиях, когда киберпреступники используют сложные технологии для обмана, возникает необходимость в более интеллектуальных инструментах защиты.

Искусственный интеллект (ИИ) и технологии машинного обучения оказываются на передовой борьбы с интернет-мошенничеством. Они могут не только обнаруживать подозрительную активность, но и прогнозировать угрозы, анализируя поведение пользователей и выявляя аномалии в данных. Эта статья рассмотрит, как ИИ применяется для выявления интернет-мошенничеств, и какие перспективы эта технология открывает для будущей борьбы с киберпреступлениями.

Виды интернет-мошенничеств

Прежде чем углубиться в применение ИИ, необходимо выделить основные виды интернет-мошенничеств, с которыми сталкиваются пользователи и компании:

1. **Фишинг –** отправка ложных сообщений с целью получения личных данных (паролей, номеров кредитных карт).
2. **Мошенничество с кредитными картами –** незаконные транзакции или кража данных карт через интернет.
3. **Атаки на социальные сети –** создание фальшивых аккаунтов или манипуляции с реальными профилями.
4. **Мошенничество в электронной коммерции** — поддельные онлайн-магазины или фальшивые предложения скидок.
5. **Злоупотребление рекламой и спам –** мошенники используют рекламу для перенаправления пользователей на вредоносные сайты.

Каждый из этих типов требует различных методов защиты и реагирования, и здесь искусственный интеллект способен предложить решения, которые гораздо быстрее и точнее обнаруживают признаки обмана.

Роль искусственного интеллекта в борьбе с интернет-мошенничествами

ИИ применяет целый ряд методов для выявления интернет-мошенничеств, используя машинное обучение, нейронные сети и другие технологии. Вот несколько ключевых направлений, в которых ИИ помогает защитить пользователей и организации от мошенничеств:

1. Анализ больших данных и выявление аномалий

Интернет-мошенничества зачастую сложно обнаружить традиционными методами, поскольку мошенники могут использовать легитимные на первый взгляд действия. Искусственный интеллект способен обрабатывать и анализировать огромные массивы данных, выявляя аномалии, которые могут указывать на мошенничество.

Например, ИИ может анализировать транзакции в реальном времени и быстро находить подозрительные операции на основании факторов, таких как необычное местоположение, время операции или сумма. Машинное обучение помогает системе учиться на предыдущих данных о мошенничествах и обнаруживать новые угрозы, которые ранее не были известны.

2. Анализ поведения пользователей

Один из самых мощных инструментов ИИ – способность выявлять необычное поведение. Машинное обучение может изучать, как пользователи обычно ведут себя на сайте или в приложении, и обнаруживать подозрительные действия. Например, если клиент всегда совершает покупки из одной страны, но вдруг выполняет операцию из другого региона или с другого устройства, система может заподозрить мошенничество.

Такой подход позволяет обнаруживать сложные формы атак, например, захват учетных записей или подмену личности, когда злоумышленник действует под видом реального пользователя.

3. Прогнозирование и предотвращение угроз

ИИ не только обнаруживает уже произошедшие мошенничества, но и способен прогнозировать потенциальные угрозы. Алгоритмы могут анализировать данные о киберугрозах и предсказывать, где и когда могут произойти атаки. Это позволяет компаниям заранее подготовиться и принять меры для предотвращения преступлений.

Например, алгоритмы могут оценивать вероятность фишинговых атак на основе анализа контента писем, которые поступают в компанию, и блокировать подозрительные сообщения еще до того, как они достигнут получателей.

4. Обнаружение фальшивых учетных записей и спам-аккаунтов

ИИ также эффективен в борьбе с созданием фальшивых учетных записей и распространением спама. Нейронные сети способны анализировать поведение новых пользователей на сайте или в социальной сети и выявлять шаблоны, характерные для ботов или мошенников. Это позволяет значительно сократить количество вредоносных аккаунтов, которые могут использоваться для мошенничеств или кибератак.

5. Улучшение безопасности онлайн-платежей

Системы ИИ активно применяются в онлайн-банкинге и электронной коммерции для улучшения безопасности транзакций. Модели машинного обучения могут оценивать риск каждой операции в режиме реального времени, сравнивая ее с историей транзакций пользователя и определенными правилами. Это позволяет блокировать подозрительные операции до их завершения, тем самым предотвращая финансовые потери.

Примеры использования ИИ для защиты от мошенничеств

Некоторые компании уже успешно применяют ИИ для борьбы с интернет-мошенничествами:

– **PayPal** использует машинное обучение для анализа транзакций в режиме реального времени. Их системы выявляют и блокируют мошеннические действия на основе анализа множества факторов, включая геолокацию, поведение пользователей и предыдущие транзакции.

– **Mastercard** и **Visa** активно используют ИИ для предотвращения мошенничеств с кредитными картами. Их алгоритмы способны в доли секунды определить вероятность того, что транзакция может быть мошеннической, и принять меры.

– **Facebook** и **Google** применяют ИИ для борьбы с фейковыми аккаунтами и рекламными мошенничествами. Их системы анализируют поведение пользователей и выявляют аномалии, которые могут указывать на неправомерные действия.

Преимущества и вызовы

Использование ИИ в борьбе с интернет-мошенничеством имеет ряд преимуществ:

– **Высокая точность**. ИИ способен быстро обрабатывать и анализировать огромные объемы данных, что делает его эффективным инструментом для обнаружения сложных схем мошенничества.

– **Автоматизация процессов**. ИИ позволяет автоматизировать многие процессы мониторинга и выявления угроз, снижая нагрузку на людей и увеличивая скорость реагирования.

– **Адаптивность**. Системы машинного обучения могут постоянно обновляться и улучшаться, чтобы справляться с новыми методами мошенничества.

Однако есть и вызовы, связанные с использованием ИИ:

– **Ложные срабатывания**. Системы ИИ могут иногда блокировать легитимные транзакции или действия, принимая их за мошеннические, что может негативно сказаться на клиентском опыте.

– **Высокая стоимость внедрения**. Разработка и поддержка ИИ-систем требуют значительных ресурсов, что может стать препятствием для небольших компаний.

– **Необходимость в защите самих ИИ-систем**. Злоумышленники могут пытаться манипулировать ИИ, обучая его неправильным данным или находя лазейки в алгоритмах.

Искусственный интеллект открывает новые горизонты в борьбе с интернет-мошенничеством, предлагая мощные инструменты для анализа данных и выявления угроз в реальном времени. Однако эта технология не является панацеей, и ее успешное применение требует сочетания интеллектуальных систем с комплексной стратегией кибербезопасности, которая включает регулярное обновление знаний о новых типах угроз и участие человека в принятии решений.

ШОХАНОВ Азамат Канатович
старший оперуполнмоченный по особо важным делам
центра по борьбе с киберпреступностью Департамента криминальной полиции МВД
Республики Казахстан капитан полиции

ИСПОЛЬЗОВАНИЕ ПОТЕНЦИАЛА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА В РЕСПУБЛИКЕ КАЗАХСТАН

С развитием цифровых технологий и увеличением числа пользователей интернета в Казахстане, проблемы интернет-мошенничества становятся всё более актуальными. Мошеннические схемы, включая фишинг, мошенничество с кредитными картами и кражу личных данных, представляют серьезную угрозу как для отдельных пользователей, так и для бизнеса. В связи с этим внедрение технологий искусственного интеллекта (ИИ) для выявления и предотвращения интернет-мошенничества становится особенно важным.

По данным аналитических компаний, Казахстан занимает высокие позиции по числу интернет-мошенничеств в Центральной Азии. С увеличением числа онлайн-транзакций и активного использования социальных сетей, мошенники находят новые способы обмана пользователей. Таким образом, необходимость в эффективных инструментах защиты, основанных на ИИ, становится всё более очевидной.

Роль искусственного интеллекта в выявлении интернет-мошенничества

1. Анализ данных

Искусственный интеллект способен обрабатывать большие объемы данных в реальном времени, что позволяет выявлять подозрительные транзакции и аномалии в поведении пользователей. Машинное обучение, в частности, может использоваться для создания моделей, которые помогают отличать легитимные действия от мошеннических.

Пример:

Системы, основанные на ИИ, могут анализировать историю транзакций и выявлять паттерны, которые указывают на мошенничество, такие как необычные суммы, частота операций или аномальные географические локации.

2. Обнаружение фишинга

Фишинг – одна из самых распространённых форм интернет-мошенничества. Алгоритмы машинного обучения могут обучаться на примерах фишинговых сайтов и электронных писем, чтобы выявлять их в будущем. Это позволяет пользователям и организациям предотвращать попадание в ловушки мошенников.

Инструменты:

Фильтры на основе ИИ, которые анализируют URL-адреса и содержимое сообщений, определяя их подозрительность на основе обученных моделей.

3. Анализ поведения пользователей

Искусственный интеллект может анализировать поведение пользователей на платфор-

мах и выявлять аномалии, которые могут указывать на мошенничество. Например, резкое изменение в привычках пользователя (внезапные крупные переводы или попытки входа из новых мест) может быть признаком взлома или мошенничества.

4. Системы биометрической аутентификации

Использование биометрических данных, таких как отпечатки пальцев, распознавание лиц или голоса, позволяет значительно повысить уровень безопасности. ИИ может анализировать биометрические данные и выявлять фальсификации, что делает доступ к важным данным и транзакциям более защищённым.

Примеры использования ИИ в Казахстане

В Казахстане уже существуют инициативы и проекты, направленные на внедрение ИИ для выявления интернет-мошенничества.

1. Финансовые технологии

Многие банки и финансовые учреждения в Казахстане начинают использовать технологии ИИ для анализа транзакций. Это помогает не только в борьбе с мошенничеством, но и в повышении качества обслуживания клиентов, позволяя быстрее выявлять и реагировать на проблемы.

2. Государственные инициативы

Правительство Казахстана активно поддерживает внедрение технологий ИИ в разных сферах. Создаются программы и платформы для повышения уровня кибербезопасности, что также включает и использование ИИ для защиты от интернет-мошенничества.

Использование возможностей искусственного интеллекта для выявления интернет-мошенничества в Республике Казахстан открывает новые горизонты для защиты пользователей и бизнеса. С учетом растущих угроз кибербезопасности, внедрение современных технологий, основанных на ИИ, становится необходимостью. Однако, для достижения максимального эффекта, важно продолжать развивать и адаптировать эти технологии к специфике казахстанского рынка, а также повышать осведомленность пользователей о возможных рисках и методах защиты.

ЕНДЫБАЙУЛЫ Ерлан
доцент кафедры кибербезопасности и информационных технологий
Алматинской академии МВД Республики Казахстан им. М. Есбулатова майор полиции

ОБНАРУЖЕНИЕ ФАЛЬШИВЫХ УЧЕТНЫХ ЗАПИСЕЙ И СПАМ-АККАУНТОВ: СОВРЕМЕННЫЕ МЕТОДЫ И ТЕХНОЛОГИИ

В эпоху цифровых технологий фальшивые учетные записи и спам-аккаунты становятся серьёзной проблемой для пользователей, компаний и социальных сетей. Эти аккаунты могут использоваться для мошенничества, распространения ложной информации, манипуляции мнением общественности и других нежелательных действий. Обнаружение и устранение таких аккаунтов требуют использования современных технологий и подходов. В данной статье мы рассмотрим методы, применяемые для выявления фальшивых учетных записей и спам-аккаунтов, а также их важность для обеспечения безопасности в интернете.

Причины появления фальшивых учетных записей.

Фальшивые учетные записи могут создаваться по различным причинам:

1. Мошенничество: Ложные аккаунты могут использоваться для обмана пользователей, например, с целью кражи личных данных или финансовых средств.
2. Распространение спама: Спам-аккаунты часто создаются для массовой рассылки рекламных сообщений или ссылок на вредоносные сайты.
3. Манипуляция общественным мнением: Фальшивые аккаунты могут использоваться для создания ложного впечатления о поддержке или антипатии к определённым событиям или личностям.
4. Вредительство: В некоторых случаях фальшивые аккаунты создаются с целью распространения ненависти или дезинформации.

Методы обнаружения фальшивых учетных записей.

1. Анализ поведения пользователей

Одним из самых эффективных способов обнаружения фальшивых учетных записей является анализ их поведения. Это может включать в себя:

– Частота публикаций: Фальшивые аккаунты часто имеют высокую частоту публикаций, которая может значительно превышать средние показатели настоящих пользователей.

– Тип контента: Спам-аккаунты могут публиковать однообразный или неуместный контент, что выделяет их на фоне других пользователей.

– Взаимодействия с другими аккаунтами: Фальшивые учетные записи могут иметь непропорционально много подписчиков или подписок, что также может служить индикатором их поддельности.

2. Алгоритмы машинного обучения

Машинное обучение и искусственный интеллект играют важную роль в обнаружении фальшивых учетных записей. Алгоритмы могут обучаться на исторических данных, выявляя паттерны и аномалии, характерные для спам-аккаунтов. Некоторые из подходов включают:

– Классификация аккаунтов: Используя наборы данных с метками «настоящий» и «фальшивый», алгоритмы могут классифицировать новые аккаунты, основываясь на их характеристиках.

– Обнаружение аномалий: Алгоритмы могут анализировать различные аспекты поведения пользователей и выявлять аномалии, указывающие на возможное мошенничество.

3. Проверка профиля

Системы могут автоматически проверять информацию, представленную в профиле пользователя. Например:

– Подтверждение личности: Запросы на подтверждение через электронную почту или SMS могут помочь подтвердить, что аккаунт принадлежит реальному человеку.

– Анализ фотографий: Использование технологий распознавания лиц может помочь выявить фальшивые учетные записи, особенно если используется изображение, взятое из открытых источников.

4. Социальный анализ

Анализ социальных сетей позволяет выявить связи между аккаунтами и оценить их достоверность. Если аккаунт взаимодействует только с другими подозрительными профилями или имеет много общих подписчиков с фальшивыми аккаунтами, это может быть признаком того, что он также является фальшивым.

Проблемы и вызовы

Несмотря на наличие современных методов и технологий, обнаружение фальшивых учетных записей сталкивается с рядом проблем:

1. Эволюция мошенничества: Мошенники постоянно совершенствуют свои методы, чтобы обходить системы обнаружения, создавая всё более правдоподобные фальшивые аккаунты.
2. Ложные срабатывания: Высокий уровень ложных срабатываний может привести к блокировке реальных пользователей, что негативно скажется на их опыте.
3. Конфиденциальность данных: Использование личной информации для анализа может вызвать вопросы о конфиденциальности и защите данных.
4. Отсутствие единых стандартов: Разные платформы могут использовать различные подходы и технологии для обнаружения фальшивых аккаунтов, что делает задачу ещё более сложной.

Обнаружение фальшивых учетных записей и спам-аккаунтов — это важная задача для обеспечения безопасности в интернете. С использованием современных методов, таких как анализ поведения пользователей, алгоритмы машинного обучения и социальный анализ, можно значительно повысить эффективность обнаружения таких аккаунтов. Однако, для успешной борьбы с этой проблемой, необходимо продолжать развивать технологии и учитывать возникающие вызовы, чтобы защитить пользователей от мошенничества и дезинформации.

ЛЕМАЙКИНА Светлана Владимировна
старший преподаватель кафедры информационного обеспечения ОВД
Ростовского юридического института МВД России

ОБЩИЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

Технология искусственного интеллекта (далее – ИИ) позволяет компьютерам имитировать человеческий интеллект и решать множественные задачи. Характеристикой искусственного интеллекта является его способность рационализировать и предпринимать действия для достижения определенной цели. Исследования в области ИИ начались в 1950-х годах и использовались в 1960-х Министерством обороны США, когда оно обучало компьютеры имитировать рассуждения человека. [1]

Общий искусственный интеллект (далее – AGI) – это раздел теоретических исследований ИИ, направленный на разработку ИИ с человеческим уровнем когнитивных функций, включая способность к самообучению. Однако не все исследователи ИИ верят, что вообще возможно разработать систему AGI. Другие термины, обозначающие AGI, включают сильный ИИ или общий ИИ. Эти теоретические формы ИИ отличаются от слабого ИИ или узкого ИИ, который способен выполнять только определенные или специализированные задачи в рамках заранее определенного набора параметров.

Учитывая, что AGI остается теоретической концепцией, мнения относительно того, как она в конечном итоге может быть реализована, расходятся. По словам исследователей искусственного интеллекта Бена Гертцеля и Кассио Пенначина, AGI относится к системам искусственного интеллекта, которые обладают разумной степенью самопонимания и автономного самоконтроля и обладают способностью решать множество сложных проблем в различных контекстах и учиться решать новые проблемы, о которых они не знали на момент их создания [2].

Большинство доступных на данный момент ИИ можно было бы отнести к категории слабых или узких ИИ, поскольку они были разработаны для решения конкретных задач и приложений. Однако стоит отметить, что эти системы ИИ по-прежнему могут быть невероятно мощными и сложными, с различными приложениями, от автономных транспортных систем до виртуальных помощников с голосовой активацией; они просто полагаются на определенный уровень человеческого программирования для обучения и точности

Поскольку AGI остается развивающейся концепцией и областью, существуют настоящие примеры AGI. Исследователи из Microsoft в сотрудничестве с OpenAI утверждают, что GPT-4 можно рассматривать как раннюю версию системы общего искусственного интеллекта. Это связано с его способностью решать новые и сложные задачи, охватывающие математику, кодирование, зрение, медицину, юриспруденцию, психологию и многое другое, с возможностями, которые по производительности близки к уровню человека [3].

Самостоятельно мыслить и обучаться – это непростая задача для общего интеллекта и она выходить за рамки поставленных задач перед ИИ. В настоящее время нет единого понимания того, когда и как именно можно создать такой интеллект, также существует много разногласий среди исследователей в этой области. Некоторые исследователи прогнозируют, что создание AGI возможно в период с 2030 по 2050 год, основываясь на текущих темпах развития ИИ. Они отмечают стремительный прогресс в таких областях, как глубокое обуче-

ние, обработка естественного языка, компьютерное зрение, которые способствуют созданию сложных и гибких систем ИИ.

Однако, другие исследователи скептически настроены в отношении создания AGI. Они подчеркивают, что человеческий интеллект является невероятно сложным и многогранным, и его полная имитация компьютером может оказаться невозможной. Хотя существуют и оптимистические прогнозы. Например, Бен Гертцель, известный специалист в области ИИ, предполагает, что создание AGI возможно уже в ближайшие десятилетия, ориентировочно к 2027-2030 годам. Он основывает свой прогноз на стремительном развитии технологий. Бен Гертцель верит, что синтез этих технологий позволит создать ИИ, способный учиться и решать задачи, сравнимые по сложности с человеческим интеллектом [4]. Несмотря на разные мнения, ясно, что создание данной технологии – эта цель требующая дальнейшего изучения и глубокого понимания как человеческого разума, так и природы интеллекта в целом.

AGI может произвести революцию практически во всех аспектах общества, от здравоохранения и образования до транспорта и развлечений. Он мог бы привести к научным прорывам, ускорить экономический рост и помочь в решении некоторых из самых насущных проблем человечества.

Данная технология AGI способна произвести революцию и в правоохранительной деятельности. Благодаря своим развитым когнитивным способностям и навыкам решения проблем AGI может значительно улучшить усилия по предупреждению преступлений и расследованию.

Решающую роль AGI может сыграть в совершенствовании стратегий предупреждения преступности. Одна из ключевых областей, где AGI может быть использован – это работа полиции на основе прогнозирования. Анализируя огромные объемы данных, включая отчеты о преступлениях, активность в социальных сетях и факторы окружающей среды, AGI может выявлять закономерности и прогнозировать потенциальные очаги преступности. Затем эта информация может быть использована правоохранительными органами для эффективного распределения ресурсов и предотвращения преступлений.

Кроме того, AGI может помочь в выявлении потенциальных угроз путем анализа различных источников данных, таких как записи с камер наблюдения, онлайн-коммуникации и данные датчиков. Автоматически обнаруживая подозрительные действия или поведение, AGI может предупреждать правоохранительные органы, позволяя им принимать быстрые меры и предотвращать преступную деятельность до того, как она произойдет.

Еще одна область, в которой AGI может внести свой вклад в предотвращение преступности, – это кибербезопасность. С ростом числа киберугроз AGI может помочь в анализе сетевого трафика, выявлении уязвимостей и обнаружении потенциальных кибератак. Благодаря постоянному мониторингу и анализу данных, AGI может предоставлять информацию в режиме реального времени и помогать в укреплении инфраструктуры безопасности.

Предоставляя передовые аналитические возможности AGI может значительно улучшить методы расследования, помогая в сборе и анализе доказательств. Преимущество AGI это его способность быстро и точно обрабатывать огромные объемы данных. Данная особенность полезна при проведении сложных уголовных расследований, где необходимо найти множество источников информации.

AGI может помочь в выявлении связей между различными доказательствами, извлечении актуальной информации из неструктурированных данных и генерации гипотез, помогающих следователям в раскрытии дел. Кроме того, AGI может использоваться в технологии распознавания лиц, что позволяет правоохранительным органам более эффективно идентифицировать подозреваемых. Анализируя черты лица и сравнивая их с большими базами данных криминального характера, AGI может обеспечить точную и быструю идентификацию, помогая в задержании преступников.

Хотя интеграция AGI в правоохранительные органы дает множество преимуществ, она также вызывает серьезные опасения. Одной из основных проблем является предвзятость алгоритмов AGI. Если данные, используемые для разработки систем AGI, предвзяты или отра-

жают негативную информацию, это может привести к искажению и созданию профилей определенных лиц и сообществ.

Еще одной проблемой является возможность неправильного использования AGI правоохранительными органами. Системы AGI должны конструироваться и реализовываться с соблюдением строгих правил и требований надзора, чтобы обеспечить их ответственное использование в соответствии с правовыми и этическими нормами. Следует будет предпринимать меры предосторожности для предотвращения несанкционированного доступа, защиты прав на частную жизнь, а также обеспечения прозрачности и подотчетности при использовании AGI.

Хотя AGI может предоставлять ценную информацию и помощь, он не должен заменять специалистов и их способность проявлять благоразумие и сочувствие в сложных ситуациях.

В России пока нет единого определения AGI. По некоторым данным, в России работают исследовательские центры по развитию искусственного интеллекта [5].

Ведутся активные разработки в этом направлении. По словам Александра Ведяхина – первого заместителя председателя правления СберБанка России, разрабатывается трехмерная модель FusionBrain учеными Института искусственного интеллекта AIRI при поддержке СберБанка. По сути это модель, которая может хорошо делать сразу много вещей: решать разные задачи, связанные с разными модальностями, такими как чтение, письмо, рисование, разговорная речь, управление физическими объектами и т.д., с использованием разных языков [6].

Общий искусственный интеллект способен произвести революцию в правоохранительных органах за счет совершенствования стратегий предупреждения преступности и методов расследования. Используя передовые когнитивные способности AGI и аналитические возможности, правоохранительные органы могут активно предотвращать преступления, выявлять потенциальные угрозы и более эффективно раскрывать сложные преступления.

Литература

1. Что такое искусственный интеллект [Электронный документ] https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp Дата ознакомления: 12.09.2024.

2. Общий искусственный интллект (AGI): определение, как это работает и примеры [Электронный документ] https://translated.turbopages.org/proxy_u/en-ru.ru.c6c10631-66e291a6-33ee3394-74722d776562/https/www.investopedia.com/artificial-general-intelligence-7563858 Дата ознакомления: 12.09.2024.

3. Что такое ChatGPT и как он приносит деньги? [Электронный документ] https://www.investopedia.com/what-is-chatgpt-7094342 Дата ознакомления: 12.09.2024.

4. Общий Искусственный интеллект (AGI) [Электронный документ] https://dzen.ru/a/Ze6iFBp3Jg7QNTzP Дата ознакомления: 12.09.2024.

5. Что такое общий искусственный интеллект и могут ли российские разработчики конкурировать с мировыми ИИ-гигантами [Электронный документ] https://rg.ru/2024/04/10/chto-takoe-obshchij-iskusstvennyj-intellekt-i-mogut-li-rossijskie-razrabotchiki-konkurirovat-c-mirovymi-ii-gigantami.html Дата ознакомления: 12.09.2024.

6. Александр Ведяхин, СберБанк: «В области ИИ Россия может стать одним из лидеров» [Электронный документ] https://www.forbes.ru/spetsproekt/481557-aleksandr-vedahin-sberbank-v-oblasti-ii-rossia-mozet-stat-odnim-iz-liderov?erid=4CQwVszH9pQPLrqovdA Дата ознакомления: 12.09.2024.

КЕБЕКПАЕВ Жасулан Серикович
технический директор компании «MSSP Global»

КИБЕРУГРОЗЫ: ОСНОВНЫЕ ВИДЫ, ПОСЛЕДСТВИЯ И МЕТОДЫ ЗАЩИТЫ

С развитием цифровых технологий и интернета киберпространство стало неотъемлемой частью нашей жизни. Оно открывает множество возможностей для бизнеса, общения и получения информации, но одновременно с этим несет значительные риски. **Киберугрозы –** это одна из самых серьезных проблем, с которыми сталкиваются как отдельные пользователи, так и организации. За последние годы количество кибератак значительно возросло, а методы злоумышленников стали более изощренными и сложными. Эта статья рассмотрит основные виды киберугроз, их последствия и эффективные способы защиты. Киберугрозы в Казахстане:

– Казахстан нас медбмом месте в глобальном рейтинге по количеству кибератак;

– Кибератак подвергались 92% казахстанских компаний

– За 2023 год злоумышленники нанесли ущерб населению и государству на 140 миллиардов тенге;

– Каждый 4 -ый смартфон заражён.

Основные виды киберугроз

Киберугрозы представляют собой любые действия или события, которые могут нарушить работу информационных систем, привести к утечке данных или нанести ущерб пользователям. Среди самых распространенных угроз можно выделить следующие:

1. Фишинг

Фишинг – это одна из самых распространенных форм кибератак, направленная на получение конфиденциальной информации, такой как пароли, данные кредитных карт или учетные данные пользователей. Злоумышленники обычно маскируются под легитимные компании или организации и рассылают фальшивые электронные письма, пытаясь заставить жертву передать свои данные. Фишинговые атаки могут быть нацелены на отдельных лиц, компании или даже на государственные учреждения.

2. Вредоносное ПО (малварь)

Вредоносное программное обеспечение, или малварь (malware), включает вирусы, трояны, шпионские программы и другие виды ПО, которое устанавливается на устройства пользователя без его ведома. Цель малвари может варьироваться – от кражи данных и блокировки системы до получения удаленного доступа к устройствам. Рансомварь (программы-вымогатели) является одной из самых опасных форм малвари, поскольку злоумышленники шифруют данные жертвы и требуют выкуп за их восстановление.

7. 3. Атаки типа «отказ в обслуживании» (DDoS)

DDoS-атаки направлены на перегрузку веб-сервера или сети путем отправки большого количества запросов. Это приводит к сбоям в работе сервера или сайта, делая его недоступным для легитимных пользователей. Такие атаки часто используются для дестабилизации работы компаний, особенно тех, чьи услуги зависят от онлайн-платформ.

4. Социальная инженерия

Социальная инженерия представляет собой форму психологического манипулирования, целью которого является получение конфиденциальной информации или доступа к системам. Злоумышленники обманывают людей, заставляя их делиться паролями, предоставлять доступ к данным или выполнять определенные действия, которые ставят под угрозу безопасность компании.

5. Кража данных

Киберпреступники часто нацелены на получение доступа к конфиденциальной информации, такой как персональные данные, финансовая информация или деловая документация. Кража данных может происходить через взлом баз данных, установку шпионского ПО или перехват сетевого трафика.

6. Атаки на интернет вещей (IoT)

С развитием Интернета вещей (IoT) возросли и риски, связанные с устройствами, подключенными к интернету. Умные камеры, бытовая техника, автомобили и другие устройства могут стать целями кибератак, если они не защищены должным образом. Злоумышленники могут использовать уязвимости в этих устройствах для доступа к сетям и данным пользователей.

Последствия киберугроз

Кибератаки могут иметь разрушительные последствия как для частных лиц, так и для организаций:

1. **Финансовые потери**. Компании могут понести значительные финансовые убытки из-за кибератак, особенно если их операции зависят от непрерывной работы информационных систем. Вымогательство (рансомварь), кража финансовых данных и другие угрозы могут обернуться прямыми потерями.
2. **Потеря данных**. Один из самых болезненных аспектов кибератак – это потеря конфиденциальных данных. Утечка личной или корпоративной информации может нанести непоправимый ущерб репутации компании и поставить под угрозу безопасность пользователей.
3. **Нарушение работы бизнеса**. Атаки типа DDoS или взлом сетей могут привести к полной остановке операций, что особенно критично для онлайн-сервисов и компаний, работающих в сфере электронной коммерции.
4. **Повреждение репутации**. Для бизнеса репутационные риски являются одними из самых серьезных последствий кибератак. Утечка данных или неспособность защитить клиентов от угроз может вызвать потерю доверия и отток клиентов.
5. **Юридические последствия**. В случае утечки данных компании могут столкнуться с судебными исками или штрафами за нарушение требований законодательства о защите данных, таких как GDPR в Европе.

Методы защиты от киберугроз

Эффективная защита от киберугроз требует комплексного подхода, включающего как технические решения, так и организационные меры. Вот несколько ключевых методов:

1. Антивирусное программное обеспечение и фаерволы

Один из базовых элементов кибербезопасности – это использование антивирусных программ и фаерволов. Антивирусы помогают обнаруживать и удалять вредоносное ПО, а фаерволы контролируют сетевой трафик, блокируя подозрительные запросы.

2. Шифрование данных

Шифрование является одной из самых надежных мер защиты данных. Даже если злоумышленникам удается получить доступ к информации, зашифрованные данные остаются недоступными для них без соответствующих ключей.

3. Аутентификация и управление доступом

Для защиты конфиденциальной информации важно использовать многофакторную аутентификацию (MFA), которая требует нескольких уровней проверки при входе в систему. Также необходимо четко регулировать доступ к данным, предоставляя его только тем сотрудникам, которым он действительно нужен для работы.

4. Обучение и повышение осведомленности сотрудников

Социальная инженерия часто становится причиной успешных кибератак. Обучение сотрудников тому, как распознавать фишинговые письма и другие формы мошенничества, поможет снизить риски. Регулярное повышение осведомленности о новых видах угроз играет важную роль в поддержании безопасности.

5. Обновление программного обеспечения и устранение уязвимостей

Обновление программного обеспечения и регулярные патчи безопасности помогают устранить уязвимости, которые могут использовать злоумышленники. Многие кибератаки направлены на старые версии программ, где обнаружены известные уязвимости.

6. Мониторинг и анализ угроз

Использование систем мониторинга безопасности (SIEM) позволяет оперативно обнаруживать и реагировать на подозрительную активность. Инструменты, основанные на искусственном интеллекте и машинном обучении, могут анализировать большие объемы данных и выявлять аномалии, которые могут быть признаком кибератаки.

Киберугрозы – это постоянная и растущая угроза в современном цифровом мире. Киберпреступники используют сложные технологии и методы для атак, и последствия их действий могут быть разрушительными как для частных лиц, так и для организаций. Однако грамотное использование технологий защиты, повышение осведомленности пользователей и внедрение эффективных процедур безопасности могут существенно снизить риски и защитить информацию. Важно понимать, что кибербезопасность – это не разовая мера, а постоянный процесс, требующий внимания, обновлений и адаптации к новым вызовам.

ДУРСУНОВ Руслан Ниязович
эксперт по информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РЕСПУБЛИКЕ КАЗАХСТАН: ВЫЗОВЫ И РЕШЕНИЯ

Информационная безопасность является важной составляющей национальной безопасности для любой страны, особенно в условиях быстрого развития технологий и цифровизации. **Республика Казахстан** активно развивает цифровую инфраструктуру, стремясь к созданию информационного общества, что делает вопросы защиты данных, систем и сетей крайне актуальными. Растущие угрозы со стороны киберпреступников и хакеров ставят перед государством задачи по обеспечению надежной защиты информационных ресурсов.

Эта статья рассматривает основные аспекты информационной безопасности в Казахстане, существующие угрозы, меры защиты и роль государственных органов в обеспечении кибербезопасности.

Основные угрозы информационной безопасности в Казахстане

Как и во многих других странах, Казахстан сталкивается с рядом киберугроз, которые могут нарушить работу государственных и частных организаций, привести к утечке конфиденциальных данных и нанести серьезный урон национальной безопасности. Среди наиболее значительных угроз можно выделить следующие:

1. Кибератаки на государственные информационные системы

Казахстан активно внедряет электронное правительство и развивает цифровые сервисы для граждан. Это делает государственные системы привлекательной целью для хакеров. Атаки на базы данных, порталы государственных услуг и информационные системы могут нарушить работу критической инфраструктуры, а также привести к утечке конфиденциальных данных граждан и государственных органов.

2. Фишинг и социальная инженерия

Фишинг – одна из самых распространенных форм интернет-мошенничества в Казахстане. Злоумышленники используют поддельные электронные письма и веб-сайты для получения доступа к личной информации пользователей. Методы социальной инженерии, такие как обман или манипуляции, направленные на получение паролей и другой конфиденциальной информации, представляют серьезную угрозу как для рядовых пользователей, так и для сотрудников государственных и частных компаний.

3. Растущая активность киберпреступников

Казахстан, как и другие страны, сталкивается с ростом активности киберпреступных группировок. Эти группы могут действовать как на международном уровне, так и локально, атакуя финансовые учреждения, компании электронной коммерции, системы онлайн-банкинга и другие секторы. Атаки на финансовые системы могут привести к утрате данных и значительным финансовым убыткам для граждан и бизнеса.

4. Уязвимость инфраструктуры интернета вещей (IoT)

С увеличением числа подключенных устройств, использующих технологии Интернета вещей, растут риски, связанные с их безопасностью. Уязвимости в устройствах IoT могут быть использованы злоумышленниками для взлома систем или сетей. В Казахстане использование умных устройств набирает обороты, что делает их потенциальными целями для атак.

5. Рансомварь и программы-вымогатели

Программы-вымогатели, или рансомварь, стали серьезной угрозой для казахстанских компаний. Злоумышленники шифруют данные и требуют выкуп за их восстановление. В случае отказа от выплаты выкупа данные могут быть уничтожены или переданы третьим лицам. Атаки с использованием рансомваря могут нарушить деятельность организаций и привести к значительным потерям.

Законодательство Республики Казахстан в области информационной безопасности

Для обеспечения информационной безопасности в Казахстане разработана система правовых актов и регуляций, направленных на защиту информации и предотвращение киберугроз.

1. Закон «О связи»

Закон регулирует вопросы защиты сетей и телекоммуникационных систем, а также устанавливает требования к безопасности информации, передаваемой по каналам связи. Он предписывает операторам связи обеспечивать защиту информации, а также внедрять меры по предотвращению несанкционированного доступа.

2. Закон «Об информатизации»

Этот закон регулирует вопросы информатизации и цифровизации в стране, устанавливая требования к обеспечению информационной безопасности в государственных информационных системах. Он также определяет обязанности государственных органов по защите данных и контролю за безопасностью цифровой инфраструктуры.

3. Закон «О защите персональных данных»

Данный закон направлен на защиту личных данных граждан. Он устанавливает обязанности организаций по сбору, хранению и обработке персональных данных, а также меры ответственности за утечку или несанкционированное использование информации.

4. Доктрина «Киберщит Казахстана»

В 2017 году правительство Казахстана приняло Доктрину «Киберщит Казахстана», которая стала стратегическим документом в области кибербезопасности. Ее цель – создание системы защиты критической информационной инфраструктуры страны от внешних и внутренних угроз, развитие потенциала в области кибербезопасности, а также укрепление сотрудничества с международными партнерами. В рамках этой доктрины разработаны планы по усилению защиты национальных информационных ресурсов и повышению квалификации специалистов в области кибербезопасности.

Государственные органы и инициативы по кибербезопасности

Важную роль в обеспечении информационной безопасности Казахстана играют государственные органы и специализированные учреждения, которые осуществляют контроль за безопасностью и противодействуют кибератакам.

1. Комитет национальной безопасности (КНБ)

КНБ играет ключевую роль в обеспечении безопасности страны, в том числе в киберпространстве. Ведомство занимается мониторингом угроз, выявлением потенциальных атак и координацией усилий по их предотвращению.

2. Национальный центр информационной безопасности (НЦИБ)

НЦИБ отвечает за защиту государственных информационных систем и баз данных. Он координирует работу по обеспечению кибербезопасности на национальном уровне, отслеживает и предотвращает угрозы, а также проводит расследования инцидентов в киберпространстве.

3. Центр анализа и расследования кибератак (ЦАРКА)

ЦАРКА является одной из ведущих организаций в области информационной безопасности в Казахстане. Центр проводит исследования и аудит систем безопасности, разрабаты-

вает рекомендации по защите данных и сетей, а также оказывает помощь организациям в предотвращении кибератак.

Меры защиты и будущее информационной безопасности в Казахстане

Для эффективной защиты информационных систем и данных в Казахстане необходим комплексный подход, включающий в себя как технические, так и организационные меры:

1. **Развитие национальных кадров в области кибербезопасности**. Для обеспечения безопасности в киберпространстве важно подготовить квалифицированных специалистов. Государственные программы должны способствовать обучению и повышению квалификации сотрудников в сфере информационной безопасности.
2. **Инвестиции в технологии кибербезопасности**. Государство и частные компании должны инвестировать в современные технологии защиты, такие как шифрование данных, многофакторная аутентификация и системы мониторинга угроз.
3. **Повышение осведомленности пользователей**. Обучение граждан и сотрудников организаций основам кибербезопасности поможет снизить риски кибератак. Важно проводить регулярные тренинги и информационные кампании, направленные на повышение уровня осведомленности о киберугрозах.
4. **Международное сотрудничество**. Учитывая глобальный характер киберугроз, Казахстан активно сотрудничает с международными организациями и другими странами для обмена информацией и совместной борьбы с киберпреступностью.

Заключение

Информационная безопасность в Республике Казахстан – это важный элемент национальной безопасности в условиях роста цифровых технологий и интернет-угроз. Внедрение современных методов защиты, подготовка кадров и усиление государственного контроля являются ключевыми факторами в обеспечении устойчивой и безопасной цифровой инфраструктуры.

МАГАЗОВ Райымбек Саламатулы
докторант 1 курса КазНУ имени Аль-Фараби

ДИПФЕЙКИ: ТЕХНОЛОГИЯ, РИСКИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

С развитием технологий искусственного интеллекта (ИИ) и машинного обучения появилось множество новых инструментов, изменяющих повседневную жизнь. Одной из таких технологий является **дипфейк –** метод создания фальшивых изображений, видео и аудио с использованием нейронных сетей. Дипфейки получили широкое распространение благодаря своей способности делать поддельные материалы практически неотличимыми от реальных, что порождает как новые возможности, так и серьезные угрозы для общества. Эта статья рассмотрит природу дипфейков, их применение, потенциальные угрозы и меры по борьбе с ними.

Что такое дипфейк?

Термин «дипфейк» (от англ. deepfake) объединяет два понятия: «deep learning» (глубокое обучение) и «fake» (подделка). Эта технология основывается на алгоритмах глубокого обучения, которые позволяют нейронным сетям анализировать и синтезировать образы и звуки, заменяя лицо или голос одного человека другим в видео или аудиофайлах. Самые распространенные виды дипфейков включают:

1. **Видео дипфейки –** замена лица или создание движений и мимики, идентичных реальным людям, в видеороликах.
2. **Аудио дипфейки –** синтез голоса, который может имитировать тембр, интонации и речь конкретного человека.
3. **Изображения –** фальсификация фотографий, на которых изменены черты лица или другие детали.

Основной механизм работы дипфейков заключается в обучении нейронных сетей на больших наборах данных, чтобы алгоритмы могли «изучить» особенности лица или голоса, а затем воспроизвести их с точностью до мелких деталей.

Применение дипфейков

Несмотря на негативные ассоциации, дипфейки имеют как положительное, так и отрицательное применение.

Положительное использование

1. **Развлечения и кинематограф**. В индустрии кино и телевидения дипфейки используются для создания спецэффектов и виртуальных персонажей. Технология позволяет «омолаживать" актеров или воссоздавать умерших звезд для новых фильмов.
2. **Образование и тренировки**. Дипфейки могут быть использованы для создания реалистичных тренингов и симуляций, например, в медицине, где можно моделировать различные клинические случаи.
3. **Искусство и творчество**. Технологии синтеза изображений и звуков открывают новые горизонты для художников и создателей контента, позволяя экспериментировать с новыми формами самовыражения.

Негативное использование

1. **Дезинформация и фейковые новости**. Одной из главных угроз является использование дипфейков для распространения дезинформации. Поддельные видео или аудио могут быть использованы для манипуляций общественным мнением, создания фальшивых новостных сюжетов или дискредитации политиков и общественных деятелей.
2. **Кибербуллинг и шантаж**. Дипфейки могут быть использованы для создания компрометирующих видео с целью шантажа или кибербуллинга. Например, подделка видео с интимным содержанием может стать инструментом давления на жертву.
3. **Мошенничество**. Киберпреступники могут использовать аудио дипфейки для обмана, подделывая голоса руководителей компаний и отдавая фальшивые распоряжения сотрудникам о переводе денежных средств.

Потенциальные угрозы дипфейков

Технология дипфейков несет значительные риски для общества. Среди основных угроз можно выделить следующие:

1. Подрыв доверия к информации

Одной из наиболее серьезных проблем, вызванных дипфейками, является потеря доверия к медиа и информации в целом. В условиях, когда каждый ролик или фотография могут быть подделаны, люди начинают сомневаться в подлинности любых материалов, что создает основу для дезинформации и политических манипуляций.

2. Влияние на политику и демократию

Дипфейки могут быть использованы для дискредитации политиков или даже подрыва избирательных процессов. Поддельные видео или аудиозаписи, в которых политические деятели якобы делают компрометирующие заявления, могут повлиять на исход выборов или вызвать социальные волнения.

3. Проблемы юридического характера

Использование дипфейков может затруднить правовую защиту жертв кибербуллинга или мошенничества. Проблемы с доказательством подлинности аудио или видеофайлов могут создать юридическую неопределенность и ослабить позиции пострадавших в судебных процессах.

4. Подрыв репутации и шантаж

Люди могут стать жертвами шантажа или клеветы через создание фальшивых видео, имитирующих компрометирующие действия. Даже если жертве удается доказать, что видео является подделкой, негативные последствия для репутации могут быть значительными.

Методы борьбы с дипфейками

С ростом угроз, связанных с дипфейками, ученые и специалисты по кибербезопасности разрабатывают различные методы борьбы с их использованием.

1. Технологии распознавания дипфейков

Существует несколько подходов к выявлению поддельных видео и изображений, основанных на анализе цифровых следов, оставленных при создании дипфейков. Например, некоторые алгоритмы могут выявлять неестественные движения глаз или мимики, которые не соответствуют реальному поведению человека.

2. Законодательные меры

Многие страны начинают вводить законы, направленные на регулирование использования дипфейков. Например, в некоторых юрисдикциях уже существуют законы, предусматривающие уголовную ответственность за создание и распространение фальшивых видео с целью обмана или шантажа.

3. Образование и повышение осведомленности

Одним из ключевых способов борьбы с дипфейками является повышение осведомленности среди населения о возможностях этой технологии и ее угрозах. Обучение людей критически относиться к потребляемой информации и проверять источники может помочь снизить воздействие фейковых материалов.

4. Разработка стандартов и этических норм

Необходимо создание международных стандартов, регулирующих использование технологий дипфейков в различных сферах, а также внедрение этических норм, направленных на предотвращение их злоупотребления.

Технология дипфейков – это мощный инструмент, который может быть использован как в благих, так и в зловредных целях. С одной стороны, она открывает новые возможности для творчества и инноваций, с другой – представляет серьезные угрозы для безопасности, приватности и доверия к информации. Для эффективной борьбы с дипфейками необходимы комплексные меры, включающие развитие технологий распознавания подделок, введение законодательных ограничений и повышение цифровой грамотности населения. Важно помнить, что в условиях стремительного развития технологий критическое мышление и осторожное отношение к информации становятся важнейшими инструментами в защите от манипуляций и обмана.

АЛИМЖАНОВА Жанна Муратбековна
профессор кафедры кибербезопасности и информационных технологий
Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к.ф-м.н.

ИНСТРУМЕНТЫ И МЕТОДЫ ОБНАРУЖЕНИЯ ДИПФЕЙКОВ

В эпоху цифровых технологий дипфейки стали серьезной угрозой аутентичности онлайн-контента. Эти сложные видеоролики, созданные искусственным интеллектом, могут убедительно имитировать реальных людей, из-за чего становится все труднее отличить правду от вымысла. Однако по мере развития технологий, лежащих в основе дипфейков, развиваются и инструменты и методы, предназначенные для их обнаружения.

Пять лучших инструментов и методов обнаружения дипфейков:

Sentinel

Рис. 1. Страж

Sentinel – это ведущая платформа защиты на основе искусственного интеллекта, которая помогает демократическим правительствам, оборонным ведомствам и предприятиям противостоять угрозе дипфейков. Технология Sentinel используется ведущими организациями Европы. Система работает, позволяя пользователям загружать цифровые мультимедиа через свой веб-сайт или API, которые затем автоматически анализируются на предмет подделки ИИ. Система определяет, является ли медиа дипфейком или нет, и обеспечивает визуализацию манипуляции.

Технология обнаружения дипфейков Sentinel предназначена для защиты целостности цифровых носителей. Он использует передовые алгоритмы искусственного интеллекта для анализа загруженного мультимедиа и определения того, были ли им манипулированы. Система предоставляет подробный отчет о своих выводах, включая визуализацию областей но-

сителя, которые были изменены. Это позволяет пользователям точно видеть, где и как манипулировали медиа [98].

Ключевые особенности Sentinel: https://thesentinel.ai/

– Обнаружение дипфейков на основе ИИ.

– Используется ведущими организациями в Европе.

– Позволяет пользователям загружать цифровые медиа для анализа.

– Обеспечивает визуализацию манипуляции.

Использование Sentinel через веб сайт или API:

Рис. 2. Загружаем цифровые медиа через веб сайт или API

Рис. 3. Система автоматически анализирует ИИ подделку

Рис. 4. Определяет, является ли это дипфейком или нет

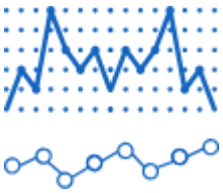


Рис.5. Показана визуализация манипуляция

Attestiv

Attestiv представила решение для обнаружения deepfake, разработанное для частных лиц, влиятельных лиц и предприятий. Эта платформа, доступная для раннего доступа, позволяет пользователям анализировать видео или социальные ссылки на видео на предмет наличия deepfake-контента. Решение Attestiv особенно актуально, учитывая растущую угрозу deepfake для рыночных оценок, результатов выборов и кибербезопасности.

Платформа использует собственный анализ ИИ для оценки и комплексного анализа поддельных элементов, точно определяя, где они находятся в каждом видео. Эта технология особенно ценна для секторов, требующих высокого уровня целостности, безопасности и соответствия, таких как банковское дело, страхование, недвижимость, СМИ и здравоохранение.

Основные характеристики платформы обнаружения дипфейков Attestiv: https://attestiv.com/deepfake-video-detection-software/

– Бесплатная базовая версия с доступными премиум- и корпоративными опциями.

– Анализирует как загруженные видео, так и ссылки в социальных сетях.

– Предоставляет оценку и подробную разбивку поддельных элементов.

– Использует запатентованную фирменную технологию искусственного интеллекта и машинного обучения.

– Рассматривает контент генеративного ИИ, замену лиц, изменения синхронизации губ и другие правки.

– Применяет уникальные «отпечатки пальцев» к видео для будущих проверок подлинности.

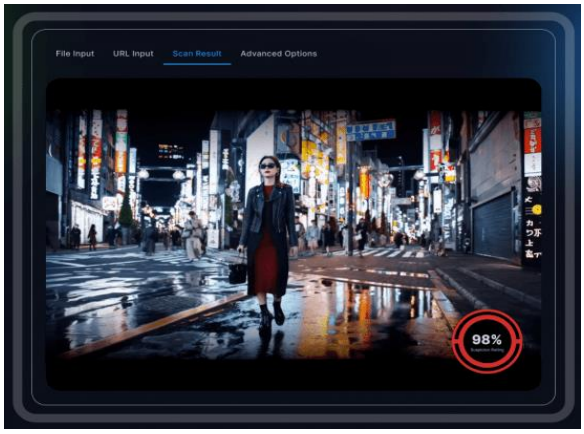


Рис. 6. Программное обеспечение Attestiv для обнаружения поддельных видео

Облачное программное обеспечение Attestiv для обнаружения deepfake-видео использует запатентованную фирменную технологию искусственного интеллекта и машинного обучения (ML) для обнаружения свидетельств фальсификации или синтетических элементов в медиафайлах. Это включает в себя deepfake, а также редактирование и другие изменения.

Процесс включает три основных этапа:

1. Загрузите видео через веб-приложение Attestiv Video или API
2. Анализ и обнаружение несанкционированного доступа
3. Проверка и отчетность

Видео захватываются и анализируются через приложение Attestiv Video или с использованием API. Процесс запускает криминалистическое сканирование, которое генерирует общий рейтинг подозрительности по шкале от 1 до 100, позволяя пользователю оценить подлинность видео.

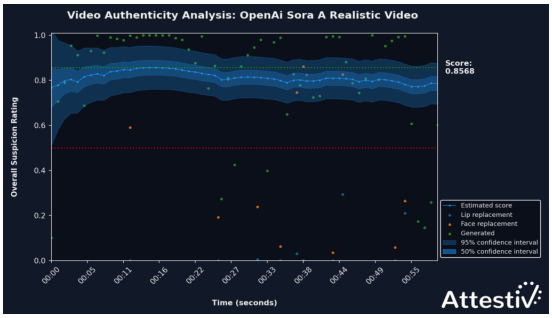


Рис. 7. Программное обеспечение Attestiv для обнаружения поддельных видео

Каждая из обученных моделей ИИ анализирует различные аспекты видео. Различные этапы процесса включают возможность проверки:

– **Контент генеративного ИИ:** Контент, созданный с использованием технологии генеративного ИИ.

– **Замена лица:** Контент, в котором лица субъектов были изменены.

– **Синхронизация губ или их замена:** контент, в котором речь и движения губ субъектов были изменены.

– **Изменения и правки** : Контент, измененный по сравнению с его первоначальной формой подозрительным образом [98].

Детектор дипфейков Intel в реальном времени

Рис. 8. Программное обеспечение FakeCatcher.

Intel представила детектор дипфейков в реальном времени, известный как FakeCatcher. Эта технология может обнаруживать поддельные видео с точностью 96%, возвращая результаты за миллисекунды. Детектор, разработанный в сотрудничестве с Умуром Чифтчи из Университета штата Нью-Йорк в Бингемтоне, использует аппаратное и программное обеспечение Intel, работает на сервере и взаимодействует через веб-платформу.

FakeCatcher ищет подлинные подсказки в реальных видео, оценивая то, что делает нас людьми – тончайший «кровяной поток» в пикселях видео. Когда наши сердца перекачивают кровь, наши вены меняют цвет. Эти сигналы кровотока собираются со всего лица, и алгоритмы переводят эти сигналы в пространственно-временные карты. Затем, используя глубокое обучение, он может мгновенно определить, является ли видео настоящим или фальшивым.

Рис. 9. Программное обеспечение FakeCatcher

Основные характеристики детектора дипфейков в реальном времени от Intel:

– Разработано в сотрудничестве с Университетом штата Нью-Йорк в Бингемтоне.
– Может обнаруживать поддельные видео с точностью 96%
– Возвращает результаты в миллисекундах
– Использует тонкий «кровяной поток» в пикселях видео для обнаружения дипфейков [98].

WeVerify

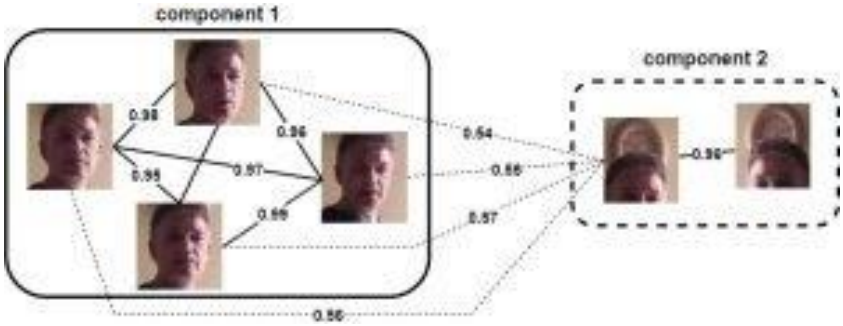


Рис.10. Программное обеспечение WeVerify

WeVerify – это проект, направленный на разработку интеллектуальных методов и инструментов для проверки контента и анализа дезинформации с участием человека. Проект

направлен на анализ и контекстуализацию социальных сетей и веб-контента в более широкой онлайн-экосистеме для выявления сфабрикованного контента. Это достигается за счет кросс-модальной проверки контента, анализа социальных сетей, микроцелевого разоблачения и общедоступной базы данных известных подделок на основе блокчейна.

Ключевые особенности WeVerify:

– Разрабатывает интеллектуальные методы и инструменты для проверки контента и анализа дезинформации с участием человека.

– Анализирует и контекстуализирует социальные сети и веб-контент

– Выявляет сфабрикованный контент посредством кросс-модальной проверки контента, анализа социальных сетей и развенчания микроцелей.

– Использует общедоступную базу данных известных подделок на основе блокчейна.

Инструмент проверки подлинности видео от Microsoft

Рис.11. Программное обеспечение Microsoft Video Authenticator Tool

Инструмент Microsoft Video Authenticator Tool – это мощный инструмент, который может анализировать неподвижное фото или видео, чтобы предоставить оценку достоверности, указывающую, были ли манипуляции с мультимедиа. Он обнаруживает границу смешивания дипфейковых и тонких элементов в градациях серого, которые не видны человеческому глазу. Он также предоставляет этот показатель достоверности в режиме реального времени, что позволяет немедленно обнаруживать дипфейки.

Video Authenticator Tool использует передовые алгоритмы искусственного интеллекта для анализа мультимедиа и обнаружения признаков манипуляций. Он ищет тонкие изменения в элементах медиа в оттенках серого, которые часто являются явным признаком дипфейка. Инструмент обеспечивает оценку достоверности в реальном времени, позволяя пользователям быстро определить, является ли носитель подлинным или нет.

Ключевые особенности инструмента Microsoft Video Authenticator:

– Анализирует неподвижные фотографии или видео.

– Обеспечивает оценку достоверности в реальном времени.

– Обнаруживает незначительные изменения оттенков серого.

– Позволяет мгновенно обнаруживать дипфейки.

Обнаружение дипфейков с использованием несоответствий фонемы и виземы

Рис.12. Обнаружение дипфейков с использованием несоответствий фонемы и виземы

Этот инновационный метод, разработанный исследователями из Стэнфордского университета и Калифорнийского университета, использует тот факт, что висемы, которые обозначают динамику формы рта, иногда отличаются или несовместимы с произносимой фонемой. Это несоответствие является распространенным недостатком дипфейков, поскольку ИИ часто изо всех сил пытается идеально сопоставить движения рта с произнесенными словами.

Техника несоответствия фонемы и виземы использует передовые алгоритмы искусственного интеллекта для анализа видео и обнаружения этих несоответствий. Он сравнивает движения рта (виземы) с произносимыми словами (фонемами) и ищет любые несоответствия. Если обнаружено несоответствие, это явный признак того, что видео является дипфейком.

Ключевые особенности обнаружения дипфейков с использованием несоответствий фонемы и виземы:

– Разработано исследователями из Стэнфордского и Калифорнийского университетов.

– Использует несоответствия между виземами и фонемами в дипфейках.

– Использует передовые алгоритмы искусственного интеллекта для обнаружения несоответствий.

– Обеспечивает четкое указание на дипфейк при обнаружении несоответствия.

Обнаружение дипфейков – это сложная, но важная задача для современного мира, где поддельные изображения и видео могут использоваться для манипуляции общественным мнением, дезинформации и подрыва доверия к информации. Использование методов машинного обучения, анализа артефактов и метаданных, а также временных алгоритмов дает возможность эффективно бороться с угрозами, связанными с дипфейками. Однако с развитием технологий генерации дипфейков требуется постоянное совершенствование инструментов для их обнаружения.

АЙТБАЕВА Рахатай Бекбергеновна
Алматы технологиялық университеті, «Ақпараттық жүйелер» кафедрасының лекторы

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ВЫЯВЛЕНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

В современном мире, где интернет-технологии проникают во все сферы нашей жизни, проблемы кибербезопасности становятся все более актуальными. Интернет-мошенничество, принимающее разные формы – от фишинга до мошенничества с кредитными картами – требует эффективных решений. Искусственный интеллект (ИИ) становится мощным инструментом в борьбе с этой проблемой, предлагая новые возможности для выявления и предотвращения мошеннических действий.

Мошенничество с использованием искусственного интеллекта уже не сценарий фантастического фильма, а наша реальность. Но не стоит забывать, что с развитием технологий, существует вопрос об их защите.

Искусственный интеллект, включая нейронные сети, имеет потенциал быть использованным как для благих, так и для недобросовестных целей.

Мошенничество с использованием голосовых генераторов: продвижение голосового синтеза и генерации реалистичных голосов с помощью нейросетей может повысить риск телефонного мошенничества. Мошенники могут использовать эту технологию для создания фальшивых голосовых сообщений или имитации голоса другого человека с целью финансовой выгоды. К примеру: Microsoft voice AI VALL-E, эта модель искусственного интеллекта преобразовывает текст в речь, точно имитируя голос человека, а образцом может служить запись продолжительностью всего в три секунды. При этом искусственный интеллект сохраняет эмоциональную окраску речи образца голоса. Даст ли это толчок развитию телефонного мошенничества? можно сказать «да». Так как мошенники зачастую первыми осваивают новые технологии и адаптируют их под свои цели.

Помимо голосовых есть риски фейковых изображений: нейросети способны генерировать реалистичные изображения на основе имеющихся фотографий. Искусственный интеллект может использовать мошенник для создания фальшивых фотографий с целью распространения ложной информации или обмана систем проверки биометрических данных.

Страшнее становится, когда, искусственный интеллект создает вредоносное программное обеспечение: участники хакерских форумов используют искусственный интеллект для написания вредоносного кода и фишинговых электронных писем. Отметим, что написать вирус могут даже те, кто не имеет опыт в программировании. Технологии искусственного интеллекта обучаются на основе того, что где-то уже существует, в дальнейшем, используя эти данные как конструктор, собирая что-то новое, избегая логических противоречий.

Действительно, с помощью социальной инженерии и нейросетей можно создать вполне правдоподобное письмо с вредоносной ссылкой. Социальная инженерия – это метод манипуляции людьми, основанный на понимании и использовании их психологических характеристик. Например, хакеры могут использовать машинное обучение для создания текстов на

основе образцов или информации из социальных сетей и других источников, чтобы сделать письмо более персональным и убедительным.

Важно понимать, что такие письма могут быть очень опасными, поскольку многие пользователи могут быть обмануты и перейти по вредоносной ссылке. Поэтому, чтобы защитить себя от таких атак, необходимо быть бдительным и не переходить по подозрительным ссылкам. Также необходимо использовать антивирусные программы и другие средства защиты, чтобы защитить свои устройства от вредоносных программ и атак.

Для защиты ваших данных и денежных средств рекомендуем придумать секретные слова или кодовые фразы, чтобы обеспечить безопасность ваших переписок и звонков. Это может быть полезно, например, если вы обмениваетесь конфиденциальной информацией или если вам нужно убедиться в том, что вы общаетесь с нужным человеком.

К примеру, если вам позвонит кто-то из близких со своего номера, будет говорить с вами своим голосом, вы не поймете, что с вами разговаривает нейросеть. И в этом весь подвох. А помогают мошенникам утекшие базы компаний, такие как доставки в Интернете, онлайн покупки и тому подобное.

Некоторые методы защиты включают использование алгоритмов проверки цифровой подписи, анализа метаданных изображений или применение алгоритмов машинного обучения для выявления аномалий и несоответствий.

Будьте бдительными, не передавайте личную информацию, если есть сомнения в подлинности звонка или сообщения. Это может помочь защитить вас и ваших близких от возможных атак со стороны мошенников и киберпреступников.

1. Основные проблемы интернет-мошенничества

Интернет-мошенничество включает в себя широкий спектр действий, направленных на обман пользователей с целью получения личной информации или денег. Основные виды мошенничества включают:

– Фишинг: Мошенники отправляют поддельные электронные письма, представляясь известными компаниями.

– Мошенничество с использованием кредитных карт: Нелегальное использование данных кредитных карт для покупок.

– Инвесторские схемы: Обман инвесторов, предлагая высокодоходные, но ненадежные инвестиции.

Эти схемы становятся все более сложными и трудными для выявления, что создает потребность в новых технологиях для защиты пользователей.

2. Как ИИ помогает в выявлении мошенничества

Искусственный интеллект может анализировать большие объемы данных и выявлять закономерности, которые сложно заметить человеку. Ниже рассмотрим ключевые методы, как ИИ применяется для борьбы с мошенничеством.

2.1. Машинное обучение

Машинное обучение (ML) – это подмножество ИИ, которое позволяет системам учиться на данных и делать прогнозы. Модели ML могут быть обучены на исторических данных о транзакциях, чтобы различать легитимные и подозрительные действия. Например:

– Классификация транзакций: Модели могут классифицировать транзакции как безопасные или рискованные на основе различных факторов (например, местоположения точки продажи, суммы и т.д.).

– Аномалия: ИИ может выявлять аномалии в поведении пользователей, которые могут указывать на мошенничество (например, резкое изменение в модели покупок).

2.2. Обработка естественного языка (NLP)

Технологии NLP позволяют ИИ анализировать текстовые данные, такие как электронные письма и сообщения. С помощью NLP системы могут выявлять фразы и паттерны, связанные с фишингом. Это позволяет:

– Автоматическое распознавание потенциального фишинга: Системы могут фильтровать подозрительные сообщения и предупреждать пользователей.

– Сентимент-анализ: Анализ настроения может помочь в выявлении манипулятивного языка, используемого мошенниками.

2.3. Постоянный мониторинг и анализ

Искусственный интеллект может предоставлять возможность постоянного мониторинга транзакций в реальном времени. Системы могут своевременно обнаруживать подозрительные действия и автоматически уведомлять о них соответствующие службы. Это особенно полезно для предотвращения мошенничества с кредитными картами.

3. Ожидаемое будущее

Несмотря на огромный потенциал использования ИИ для выявления интернет-мошенничества, важно помнить, что мошенники также могут использовать новые технологии для улучшения своих схем. Поэтому нужно продолжать развивать и адаптировать методы ИИ, обеспечивая постоянное обновление алгоритмов и систем безопасности.

Применение искусственного интеллекта для выявления интернет-мошенничества представляет собой многообещающий путь к повышению кибербезопасности. Использование машинного обучения и обработки естественного языка позволяет компаниям оперативно реагировать на угрозы и защищать пользователей от потерь. В условиях быстро меняющегося цифрового ландшафта, усилия по интеграции ИИ в системы безопасности станут ключевыми для успешной борьбы с мошенничеством в интернете.

ТАСБУЛАТОВ Руслан Ермекович
магистрант 2 курса факультета послевузовского образования Алматинской академии МВД Республики Казахстан им. М. Есбулатова капитан полиции

ТЕХНОЛОГИЯ ИССКУСТВЕННОГО ИНТЕЛЛЕКТА В РАСКРЫТИИ И ИЗОБЛИЧЕНИИ ИНТЕРНЕТ ПРЕСТУПЛЕНИЙ

Глобализация и развитие информатизационного общества быстрыми темпами влияют на облик современного цифрового мира. Цифровая сфера стала прочно укоренятся в нашей жизни и становится системообразующим фактором и охватывает все отрасли науки и технологий и стали значимыми, как и вся инфраструктура в любом направлении. Новейшие технологии дают перспективу каждому человеку возможность быть вовлеченным в глобальное цифровое пространство, что совершенствует международное взаимопонимания и построению общества основанному на знаниях информированных граждан. С развитием цифровых технологий, как и в любой другой сфере присутствует и обратная сторона. Цифровой мир позволяет все больше и больше нашей личной информации храниться в интернете, что дает новые возможности преступной деятельности криминальной среде. По мере развития информационных систем юридические и этические направления стали отставать от новых разработок. В связи с данной ситуацией и изучения тенденций киберпреступности и их последствий законодателистали принимать обоснованные решения о регулировании технологий и защищать людей от киберугроз посредством исскуственного интеллекта.

В Казахстане внедрена IT-разработка с элементами искусственного интеллекта (ИИ), которая позволяет по камерам видеонаблюдения находить людей, даже если их внешность изменилась. Правоохранительные органы усилила надзор за розыском лиц, скрывающихся от правосудия. Мониторя камеры видеонаблюдения в местах массового скопления людей, уже смогли распознать и задержать 53 беглецов. Теперь к этой работе подключили ИИ, который пока используется только в двух городах – Алматы и Атырау. ИИ позволяет распознавать лица разыскиваемых граждан даже с учетом изменения их внешности или возраста. В частности, это может быть полезно для поиска людей, которые изменили внешность намеренно или просто с течением времени. С августа в Алматы и Атырау правоохранительные органы подключили свою IT-разработку с элементами искусственного интеллекта к камерам видеонаблюдения для автоматического распознавания беглых преступников, должников и пропавших без вести. За два дня удалось установить двоих человек, скрывающихся от следствия, и двоих пропавших. Генеральный прокурор поручил внедрить эту систему распознавания лиц во всех регионах страны [1].

*«*Исскуственный интеллект оказывает глубокое влияние на технологические продукты и все аспекты управления продуктами. Менеджерам по продуктам и предложениям крайне важно изучить, как исскуственный интеллект может помочь им сделать большие шаги к улучшению своего ценностного предложения уже сейчас*»,* – Генеральный директор Центра поддержки цифрового правительства Рустем Бигари.

Как оператор национальной платформы искусственного интеллекта, АО «НИТ» будет играть центральную роль в развитии и интеграции ИИ-технологий в различные сектора экономики Казахстана.

Платформа ИИ предназначена для создания моделей, хранения разработанных дата сетов, также предоставления MLOPS инструментов и вычислительных мощностей. Национальная платформа искусственного интеллекта – это не просто технологическая инфраструктура, это катализатор для инноваций и развития, который принесет Казахстану ведущие позиции в области искусственного интеллекта в регионе.

В настоящее время ведется активная работа по созданию архитектуры платформы ИИ, разработке ее компонентов, тестированию и подготовке документации. АО «НИТ» будет предоставлять платформу ИИ государству, бизнесу, науке, образованию для разработки и реализации инновационных решений на основе искусственного интеллекта, которые будут способствовать развитию автоматизации процессов, улучшению качества и доступности государственных и коммерческих услуг.

«Суперкомпьютер – это серверные мощности, которые работают по несколько другим технологиям на базе технологии видеокарт. Они будут размещены в Центре обработки данных АО «Национальные информационные технологии». Уже вся необходимая инфраструктура подготовлена. До конца года данный суперкомпьютер будет запущен. Мощности данного суперкомпьютера будут предоставляться как госсектору, так и научным организациям. В том числе мы планируем поддерживать через предоставление серверных мощностей суперкомпьютера стартапы и бизнес-сообщества. Национальная платформа искусственного интеллекта будет предоставляться в качестве инструментария, площадки для создания новых продуктов, новых систем с использованием ИИ», – отметил Председатель правления АО «НИТ» Ростислав Коняшкин [2].

Правоохранительные органы Казахстана отмечают все более широкое использование интернета для распространения наркотиков, что требует применения современных технологий, в том числе искусственного интеллекта, для пресечения данного рода преступлений, заявил министр внутренних дел РК Марат Ахметжанов. Так, каждое седьмое зарегистрированное в 2023 году противоправное деяние, связанное с наркотическими веществами, происходит в онлайн-пространстве, передает слова министра на заседании правительства Казахстана информационное агентство «Казинформ».

«Конечно, нами блокируются такие интернет-магазины. В этом году их число составило 604. Однако данная мера не решит проблему кардинально», – сообщил Ахметжанов, добавив, что постоянно возникают новые сайты, выявление которых занимает длительное время. При этом, уточнил министр, организаторы таких сайтов находятся за пределами Казахстана. «Для перекрытия такого незаконного контента необходимо современное аппаратно-программное оборудование. В этой связи комплексным планом борьбы с наркоманией и наркобизнесом предусмотрено обеспечение соответствующими средствами («Аргус», «Айрис», «Тритон»). Они позволят автоматизировать выявление фактов распространения наркотиков через социальные сети и сайты. Также система «Кибернадзор» обеспечит блокировку сайтов в онлайн-режиме. То есть искусственный интеллект сам выявляет и немедленно блокирует. Одновременно с этим он способствует установлению пользователей и организаторов таких сайтов», – указал руководитель казахстанского МВД. В целях установления мест посевов конопли и обнаружения нарколабораторий также применяются технические средства в виде дронов, оснащенных, в том числе, газоанализаторами, указал Ахметжанов [3].

Мошенничество с использованием искусственного интеллекта уже не сценарий фантастического фильма, а наша реальность. Но не стоит забывать, что с развитием технологий, существует вопрос об их защите. Искусственный интеллект, включая нейронные сети, имеет потенциал быть использованным как для благих, так и для недобросовестных целей.Мошенничество с использованием голосовых генераторов: продвижение голосового синтеза и генерации реалистичных голосов с помощью нейросетей может повысить риск телефонного мошенничества. Мошенники могут использовать эту технологию для создания фальшивых голосовых сообщений или имитации голоса другого человека с целью финансовой выгоды. К примеру: Microsoft voice AI VALL-E, эта модель искусственного интеллекта преобразовывает текст в речь, точно имитируя голос человека, а образцом может служить запись продолжительностью всего в три секунды. При этом искусственный интеллект сохраняет эмоциональную окраску речи образца голоса. Даст ли это толчок развитию телефонного мошенничества? можно сказать «да». Так как мошенники зачастую первыми осваивают новые технологии и адаптируют их под свои цели.

Помимо голосовых есть риски фейковых изображений: нейросети способны генерировать реалистичные изображения на основе имеющихся фотографий. Искусственный интеллект может использовать мошенник для создания фальшивых фотографий с целью распространения ложной информации или обмана систем проверки биометрических данных. Страшнее становится, когда, искусственный интеллект создает вредоносное программное обеспечение: участники хакерских форумов используют искусственный интеллект для написания вредоносного кода и фишинговых электронных писем. Отметим, что написать вирус могут даже те, кто не имеет опыт в программировании. Технологии искусственного интеллекта обучаются на основе того, что где-то уже существует, в дальнейшем, используя эти данные как конструктор, собирая что-то новое, избегая логических противоречий.

Действительно, с помощью социальной инженерии и нейросетей можно создать вполне правдоподобное письмо с вредоносной ссылкой. Социальная инженерия - это метод манипуляции людьми, основанный на понимании и использовании их психологических характеристик. Например, хакеры могут использовать машинное обучение для создания текстов на основе образцов или информации из социальных сетей и других источников, чтобы сделать письмо более персональным и убедительным.

Важно понимать, что такие письма могут быть очень опасными, поскольку многие пользователи могут быть обмануты и перейти по вредоносной ссылке. Поэтому, чтобы защитить себя от таких атак, необходимо быть бдительным и не переходить по подозрительным ссылкам. Также необходимо использовать антивирусные программы и другие средства защиты, чтобы защитить свои устройства от вредоносных программ и атак. Для защиты ваших данных и денежных средств рекомендуем придумать секретные слова или кодовые фразы, чтобы обеспечить безопасность ваших переписок и звонков. Это может быть полезно, например, если вы обмениваетесь конфиденциальной информацией или если вам нужно убедиться в том, что вы общаетесь с нужным человеком. К примеру, если вам позвонит кто-то из близких со своего номера, будет говорить с вами своим голосом, вы не поймете, что с вами разговаривает нейросеть. И в этом весь подвох. А помогают мошенникам утекшие базы компаний, такие как доставки в Интернете, онлайн покупки и тому подобное. Некоторые методы защиты включают использование алгоритмов проверки цифровой подписи, анализа метаданных изображений или применение алгоритмов машинного обучения для выявления аномалий и несоответствий [4].

В современном мире, где цифровые технологии играют все более важную роль, онлайн мошенничество становится одной из самых серьезных проблем, с которым потребители сталкиваются ежедневно, в том числе в сети Интернет. Онлайн мошенничество затрагивает не только отдельных пользователей, но и организации, правительства и оказывает значительное влияние на мировую экономику. Те, кто стал жертвой мошенничества, сообщают об эмоциональном смятении, стыде и потере уверенности. Интернет-мошенничество является одним из наиболее заметных проявлений цифрового вреда для потребителей, причиняя потребителям финансовый, эмоциональный и психологический вред. Однако, с развитием искусственного интеллекта (ИИ), появляется возможность борьбы с этой проблемой более эффективными методами.

Ежегодно 15 марта потребительское движение отмечает Всемирный день прав (WCRD), повышая глобальную осведомленность о правах потребителей, их защите и расширении прав и возможностей. Во всех странах началась работа по повышению прозрачности и ответственности систем искусственного интеллекта (ИИ), а тема текущего года заявлена как «Справедливый и ответственный ИИ для потребителей».

«Во всем мире интернет-мошенничество растет, но глобальные технологические компании не могут обнаружить и предотвратить мошенничество на своих платформах. Мошенники используют слабую защиту платформы для нападения на потребителей через социальные сети, онлайн-рекламу, торговые площадки и обмен сообщениями. Эти мошенничества часто являются изощренными, узконаправленными и их трудно обнаружить потребителям» [ООН, WCRD, 2023]. Поэтому:

1. ИИ предоставляет уникальные возможности для обнаружения и предотвращения онлайн мошенничества. За счет своей способности обрабатывать и анализировать огромные объемы данных, ИИ может распознавать аномалии и необычные паттерны, которые могут свидетельствовать о мошеннической деятельности. В дополнение к этому, ИИ может учиты-

вать контекст и комбинировать различные данные для построения более точных моделей оценки риска на платформах компаний и в социальных сетях.

2. Одной из областей, где ИИ может дать значительный вклад в борьбе с мошенничеством, является финансовая сфера. Банки, платежные системы и другие финансовые учреждения активно используют ИИ-технологии для обнаружения мошеннических операций. Алгоритмы машинного обучения, основанные на исторических цифровых данных, позволяют выявлять необычные транзакции или подозрительное поведение, что помогает предотвратить возможные финансовые потери. Согласно отчету «Глобальное состояние мошенничества» (2023г.) менее 1 из 10 жертв во всем мире успешно возвращают деньги, потерянные в результате мошенничества, а потребители в странах с низким и средним уровнем дохода наиболее уязвимы.

3. ИИ также может применяться для борьбы с мошенничеством в сфере электронной коммерции (торговли и предоставления услуг населению). Автоматические системы могут анализировать данные о покупателях и их поведении для определения потенциально мошеннических заказов. Используя различные параметры, такие как связь между покупателем и продавцом, историю покупок и другие характеристики, ИИ может выявлять попытки обмана и предотвращать возможные убытки для бизнеса.

4. Также следует упомянуть о роли ИИ в сфере кибербезопасности. ИИ может быть использован для обнаружения и предотвращения кибератак. Анализируя поведение в цифровом пространстве, ИИ может идентифицировать атаки и предлагать соответствующие меры по их предотвращению. Благодаря ИИ, программисты могут создать более безопасное онлайн-пространство и защитить пользователей от потенциальных угроз.

5. Однако, необходимо учитывать некоторые этические и юридические аспекты применения ИИ в борьбе с онлайн мошенничеством. Важно обеспечить прозрачность и ответственность в использовании алгоритмов ИИ, чтобы избежать возможного нарушения прав и неправомерного использования персональных данных. Также стоит учитывать, что мошенники становятся все более изобретательными и адаптивными, и поэтому необходимо непрерывно развивать и совершенствовать методы борьбы с ними.

Чтобы предотвратить мошенничество, все доступные технологические платформы, используемые человеком, должны обеспечивать защиту его прав, в том числе иметь расширенные процедуры проверки (например, при авторизации пользователя), строго соблюдать рекламную политику и взаимодействовать с другими службами и органами власти по запросу. Чтобы вовремя обнаружить и пресечь мошенничество, когда оно происходит, необходимы: передовые системы мониторинга; оперативное удаление контента; образование и осведомленность потребителя, а также службы поддержки или «горячая линия». Применение искуственного интеллекта в борьбе с мошенничеством открывает новые возможности для обнаружения и предотвращения преступных действий в онлайн-среде. Однако необходимо развивать эти технологии таким образом, чтобы они соответствовали этическим и юридическим принципам и обеспечивали безопасность и конфиденциальность пользователей в интернете. Только так мы сможем достичь значительного прогресса в борьбе с онлайн мошенничеством и создать более безопасную и доверительную цифровую среду для граждан (населения) [5].

Своевременное межгосударственное уведомление о хакерских атаках будет способствовать меньшему распространению вредоносных программ и уменьшению количества пострадавших, поэтому участникам БРИКС (организация государств Бразилия, Россия, Индия, Китай, Южноафриканская Республика) стоит задуматься над проработкой этого вопроса, считает член Совета по правам человека – по развитию гражданского общества и правам человека, гендиректор АНО «Белый Интернет» Элина Сидоренко. «Суверенное киберпространство невозможно без наличия диалога с партнерами и соседями. Задачи обеспечения цифрового суверенитета и усиление международного сотрудничества в борьбе с киберпреступниками дополняют, а не противоречат друг другу. Важным элементом защиты суверенного киберпространства должен стать обмен информацией для укрепления мер защиты как внутри стран, так и в рамках международной кооперации», – подчеркнула Сидоренко в ходе IX Юридического форума стран БРИКС. Она обратила внимание, что сегодня большее количество атак совершается непосредственно на регион, а не отдельную страну. Сидоренко привела в пример недавно обнаруженный сингапурской Group IB, новый вредоносный ПО

для Android по названием Ajina.Banker: он распространялся через Telegram под видом легитимных приложений для банков, платежных систем, госуслуг или коммунальных услуг. Пострадала преимущественно клиентура банковского сектора таких стран как Армения, Азербайджан, Исландия, Казахстан, Кыргызстан, Пакистан, Россия, Таджикистан и Узбекистан, рассказала глава «Белого Интернета». «Вполне вероятно, что своевременное получение уведомлений от соседних стран, где были обнаружены первые случаи атак, способствовало бы меньшему распространению вредоноса и уменьшению количества пострадавших», – считает Сидоренко. «Поэтому целесообразно принятие региональных соглашений о создании Координационных центров, в чьи задачи будет входить налаживание активной коммуникации между дружественными странами для своевременного устранения угроз и внедрения единых сквозных стандартов цифровой безопасности. Сегодня на пространстве БРИКС создан специальный электронный реестр для обмена данными о компьютерных атаках и инцидентах, однако, важно работать с компаниями и людьми стран региона», - указала профессор. Ключевым в вопросе обеспечения цифровой безопасности является человеческий фактор. «И работа по внедрению правил цифровой гигиены также должна вестись скоординированно. Это может способствовать снижению ущерба от цифровых преступлений», - резюмировала член Совета по правам человека [6].

В заключение мы можем резюмировать то что исскуственный интеллект обладает огромными возможностями ,такие как автоматизация ежедневных задач, анализирование огромных данных, улучшение пользовательского навыка и может обучаться на основе данных, что позволяет ему адаптироваться к изменениям и предсказывать тренды. В связи с необходимостью качественных данных и проблемы с интерпретируемостью решений исскуственного интеллекта и этических моментов его применения необходимо развивать и максимизировать его пользу и минимизировать риски. Исскуственный интеллект трансформирован во все сферы жизни человека, улучшая качество жизни, и открывает новые горизонты для инноваций.

Литература

1. Казахстан внедряет искусственный интеллект для поиска разыскиваемых лиц.https://smartnews.kz/ru/news/12918-kazahstan-vnedryaet-iskusstvennyj-intellekt-dlya-poiska-razyskivaemyh-lits (интернет источники, дата обращения 19.09.2024год).

2. Представители Минцифры рассказали о дальнейшем использовании исскуственного интеллекта. https://www.gov.kz/memleket/entities/mdai/press/news/details/742959?lang=ru (интернет источники, дата обращения 19.09.2024год).

3. МВД Казахстана применит исскуственный интеллект для борьбы с наркотиками. http://rapsinews.ru/international_news/20230314/308745931.html (интернет источники, дата обращения 19.09.2024год).

4. Исскуственный интеллект и мошенники. https://cgon.rospotrebnadzor.ru/naseleniyu/gramotnyy-potrebitel/ii-protiv-onlayn-moshennichestva/ (интернет источники, дата обращения 19.09.2024год).

5. ИИ против онлайн мошенничества. https://cgon.rospotrebnadzor.ru/naseleniyu/gramotnyy-potrebitel/ii-protiv-onlayn-moshennichestva/ (интернет источники, дата обращения 19.09.2024год).

6. Кибербезопасность, Юридический форум стран БРИКС, «, БРИКС, Элина Сидоренко, Москва, Россия http://rapsinews.ru/digital_law_news/20240919/310253277. html (интернет источники).

БЕЙСЕНБІ Арна
Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы
жоғары оқу орнына кейінгі білім беру факультетінің
2 курс магистранты полиция аға лейтенанты

КИБЕРБУЛЛИНГ: ОНЛАЙН ҚОРҚЫТУ ЖӘНЕ ҚОРЛАУ ҮШІН ЖАУАПКЕРШІЛІК МӘСЕЛЕЛЕРІ

Кибербуллинг – бұл қазіргі заманда өсіп келе жатқан проблеманың бірі, ол құрбандар үшін де, қылмыскерлер үшін де үлкен проблемалар болуы мүмкін. Бұл платформалар, әлеуметтік желілер және ұялы телефондар сияқты сандық құралдарды қолдану, қорқыту немесе адамдарға зиян келтірудің басқа тәсілдерін қолдануды білдіреді. Кибербуллинг әр түрлі формада болуы мүмкін, соның ішінде зұлымдық немесе қауіп төндіретін хабарламалар жариялау, жалған ақпараттар тарату, ұятты фото-, видео-мазмұнмен бөлісу немесе интернеттегі әлеуметтік топтардың кез-келгенін алып тастау.

Кибербуллингтің салдары адамдарға айтарлықтай зиян келтіруі мүмкін. Зардап шеккен адамдарда мазасыздық, депрессия, өзін-өзі бағалаудың төмендеуі және суицидтік ойлар белгілері болуы мүмкін. Балалардың 75%-ы интернетте түрлі қауіп-қатерлерге тап болуда. Мұны ESET антивирустық компаниясы жазғы каникул қарсаңында интернет - пайдаланушылардан сұхбат алу арқылы анықтады. Сонымен қатар, олар ұйқы, тәбет, зейін қою және басқа да проблемаларға тап болуы мүмкін. Кейбір жағдайларда кибербуллинг физикалық зардаптарға әкелуі мүмкін, өйткені адам оқшаулануды сезінуі немесе өзіне қауіп төндіруі мүмкін.

2022 жылы 143 жасөспірім өз-өзіне қол жұмсады, ал 306 кәмелетке толмағандар интернет кеңістігінде қорлау салдарынан өз-өзіне қол жұмсамақ болды. Кибербуллингпен айналысатын адамдар да жағымсыз салдарға ұшырауы мүмкін. Кибербуллинг қорқытуға қарағанда сирек кездеседі. Жалпы, жасөспірімдердің 5%-ы кибербуллингтің құрбаны болды немесе айына 2-3 рет немесе одан да көп басқа адамдардың кибербуллингіне қатысқан. Жасөспірімдердің 12%-ы кем дегенде бір рет кибербуллингке ұшыраған. Егер олардың әрекеттері қылмыстық деп танылса, олар заңды салдарға, сондай-ақ олардың беделіне нұқсан келтіру, достар табу немесе жұмыс табу қиындықтары сияқты әлеуметтік және кәсіби салдарға тап болуы мүмкін.

Зерттеушілердің зерттеу нәтижелері көрсеткендей кибербуллингке тап болған респонденттердің үштен бірінен астамы жеке хабарламаларда қорлық көрген, 24%-ы өздері туралы жағымсыз жазбаларды көрген, ал үштен бір бөлігі – 31%-ы фотосуреттерінің астында жағымсыз пікірлерді оқыған. Кибербуллингті азайтудың бір жолы-адамдарға олардың әрекеттерінің салдары туралы хабарлау. Мұны ата-аналар мен мұғалімдерге арналған халықты ақпараттандыру науқандары, білім беру бағдарламалары және ресурстар арқылы жасауға болады. Кибербуллингтің салдары туралы ақпаратты хабардар етуді арттыру, адамдар мұндай мінез-құлыққа барар алдында ойлануы мүмкін.

Кибербуллингті азайтудың тағы бір жолы-зардап шеккендерге қолдау мен көмек беру. Қолдау мен көмек беруге кеңес беру, терапия, сондай-ақ кибербуллинг жағдайлары туралы хабарлау және олардың салдарын жою тетіктері кіруі мүмкін. Осы құралдардың арқасында жәбірленушілер өздерін сенімді сезініп, әрекет ете алады және көмек сұрай алады. Кибербуллинг әрекеттері үшін жауапкершілікке тарту да маңызды. Бұл кибербуллингпен

айналысатын студенттерге тәртіптік жаза қолдануды немесе мұндай мінез-құлық қылмыстық деп саналатын жағдайларда сот ісін жүргізуді қамтуы мүмкін. Кінәлілерді жауапқа тарту арқылы бұл кибербуллингке жол берілмейтінін және ауыр зардаптарға әкелуі мүмкін екенін анық көрсетеді. Біздің қоғамымызда құрмет пен мейірімділік мәдениетін қалыптастыру маңызды. Бұған мейірімділік пен жанашырлық сияқты жағымды мінез-құлықты ынталандыру және осы мінез-құлықты өз бетінше модельдеу арқылы қол жеткізуге болады. Құрмет пен мейірімділік мәдениетін құру арқылы біз барлығына қонақжай орта жасай аламыз.

Кибербуллинг (ағылшын сөзінен bull-бұқа, яғни мағынасы агрессивті шабуыл, қорлау, арандату) – бұл қасақана, жүйелі агрессивті жәбірленушіге қарсы бір адамның немесе бір топтың лездік хабар алмасу қызметтері арқылы, сондай-ақ әлеуметтік желілер, web-сайттар, электрондық пошта, мобильді байланыс арқылы жүзеге асырылатын, жәбірленушіге келтіретін психологиялық зиян.

Американдық ғалымдар кибербуллингтің үш ерекшелігін бөліп, оларды үш А принципі деп атады:

– *A-anonymous (анонимділік)*

– *A-accessible (қолжетімділік)*

– *A-affordable (төменбаға).*

Анонимдік кибербуллинг орындаушы үшін әлдеқайда оңай,себебі ол жәбірленушінің сол сәттегі нақты реакциясын көрмейді.Қылмыскер ол хабарламаларды тірі адам оқып отырғанын ұмытып кетеді.

Қазіргі уақытта интернеттің қолжетімді болғандықтан, мобильді құрылғылар мен сымсыз желілер әсерінен, тұтынушыға әлеуметтік желілерде сөйлесу тәулігіне 24 сағат, аптасына 7 күн мүмкіндік береді. Бұл қылмыскерге негізгі жұмысын тоқтатпай жұмыс жасап, алаңдамауға жағдай жасайды.

Кибербуллинг тікелей және жанама болуы мүмкін.

Тікелей кибербуллинг-жәбірленушіге хаттар арқылы тікелей шабуыл жасау хабарламалар.

Жанама кибербуллинг-бұл процеске басқа адамдардың олардың келімісіз арқылы қатысуы.

Р. Ковальски және С. Лимбер кибербулингтің келесі түрлерін ажыратады: Флейминг (flame – «жалын») – бұл қудалаудың түрінде адамдар қарапайым балағаттаудан басталып, эмоционалды әңгімеге дейін апаруы мүмкін. Және бұл процесс көпшілік арасында өтеді.

(Пікірлер, форумдар).

Кибералкинг (киберқылмыс) – әртүрлі қауіп-қатерлері туғызатын хабарламалар, және жеке деректерді керісінше ,жәбірленушіге зиян келтіретіндей пайдалану.

Секстинг – жәбірленушілінің беделін түсіру мақсатында, жеке фотосуреттер мен видеоларды тарату.

Жалған парақшаларды бұзу және жасау – жалған ақпаратты жариялау.

Троллинг-әртүрлі эмоция туғызу үшін жіберілетіг арандатушылық хабарламалар немесе түсініктемелер.

Ескермеу (елемеу) – топтардан, әртүрлі форумдардан, қауымдастықтардан шығу.

Кибербуллинг кейде байқаусызда болуы мүмкін. Мысалы, жабық топтың немесе онлайн-қауымдастықтың бір мүшесі сәтсіз әзілдеуі.

Қазіргі таңда Қазақстан Республикасы Парламенті Мәжілісі депутаттарының бастамасы бойынша кейбір заңнамалық актіге бала құқықтарын қорғау мәселелері бойынша өзгерістер мен толықтырулар енгізу әзірленіп жатқанын атап өткеніміз жөн. ҚР Ақпарат және қоғамдық даму министрлігі БАҚ саласындағы мемлекеттік саясат департаменті директорының орынбасары Әлішер Мұқажан заң жобасы шеңберінде балалардың құқықтарын қорғауды күшейтуге, «онлайн оқыту» ұғымын енгізуге және басқа да онымен байланысты құқықтық қатынастарды орнатып, «буллинг» пен «кибербуллинг» ұғымын құқықтық бекітуге бағытталған бірқатар кодекс пен заңға өзгерістер мен толықтырулар енгізу жоспарланғанын жеткізді.

Білім беру ұйымы кәмелетке толмағанды қудалау (буллинг) фактілерінің алдын алуда барлық профилактика субъектілерімен өзара іс-қимылды мынадай жолдар арқылы жүзеге асырады:

1) кәмелетке толмағанды жәбірлеудің (буллингтің) профилактикасы бойынша білім беру ұйымының ішкі жоспарын әзірлеу және қабылдау;

2) баланы жәбірлеудің (буллингтің) барлық фактілерін анықтау және тіркеу;

3) жағдайды кешенді бағалауды, баланың құқықтары туралы құқықтық білімді және жеке жұмыс жоспарын әзірлеуді қамтитын жәбірлеуге (буллингке) ұшыраған балаға психологиялық қолдау мен көмек көрсетуді ұйымдастыру;

4) жағдайды кешенді бағалауды, міндеттері мен заңды жауапкершілігі, жәбірлеудің (буллингтің) туралы құқықтық білім беру және агрессорды оңалту және қайта әлеуметтендіруді қамтитын жәбірлеудің (буллингтің) агрессор баланы психологиялық-педагогикалық сүйемелдеуді ұйымдастыру;

5) балаларды жәбірлеу (буллинг) фактілері бойынша арнайы қызметтерге жүгіну мүмкіндігі туралы хабардар ету;

6) ІІО-ны, кәмелетке толмағандардың істері және олардың құқықтарын қорғау жөніндегі комиссияны (бұдан әрі – КТҚЖК), қорғаншы және қамқоршы органдыдереу хабардар ету, сондай-ақ мүдделі мемлекеттік органдарға жәбірлеу (буллинг) ұшыраған бала туралы ақпарат беру;

7) жәбірлеудің (буллингтің) профилактикасына бағытталған іс-шараларды ұйымдастыру және білім беру ұйымдарында қолайлы моральдық ахуал қалыптастыру

8) балаларға қатысты жәбірлеу (буллинг) фактілері туралы өтініштерді қарау, олардың жолын кесу жөнінде шаралар қабылдау;

9) жәбірлеуге (буллингке) зардап шеккен білім алушыларға көмек көрсету үшін өз құзыреті шеңберінде басқа органдар мен ұйымдарды тарту;

10) ата-аналардың (заңды өкілдердің) ата-ана құқықтарын теріс пайдалану жағдайлары туралы білім беруді басқару органдарын және ІІО-ны, БП КДН-ны жазбаша хабардар ету шараларын қабылдау;

11) зардап шеккен кәмелетке толмаған баланың құқықтары мен мүдделерін бұзуға ықпал ететін себептер мен жағдайлар жойылған жағдайда жәбірлеу (буллинг) фактісі жеке жағдайды жабу туралы шешім қабылдаған жағдайларда тоқтату;

12) жәбірлеу (буллинг) жағдайлары туралы статистикалық деректерді, оның ішінде қайталап жіберу және қабылданған шаралар туралы ақпаратты аумақтық білім басқармасына тоқсанына кемінде 1 рет жолдау.

13) Жәбірлеуге (буллингке) ұшыраған баламен жұмыс істеудің жеке жоспарына төмендегілер кіреді:

Арессорлармен жұмыс: агрессормен әңгімелесу және мектептің әлеуметтік педагогтарының отбасына бару; баланың ата-анасын немесе заңды өкілдерін жәбірлеу (буллинг) туралы хабардар ету, баланың коммуникативтік қабілеттерінің сапасын арттыруға жеке және топтық бейімдеу; эмоционалды-мінез-құлық көріністерін бақылау дағдыларын қалыптастыру; кез келген адамнның адам құқықтарына, ар-намысы мен абыройына құрметпен қарауды қалыптастыру; позитивті тәрбие, балалармен қарым-қатынас, басқа балалармен тұлғааралық қарым-қатынасты қалыптастыру бойынша нормаларды түсіндіру бойынша жеке кездесулер өткізу; жәбірлеуге (буллингке) ұшыраған баламен жұмыс: баланы қызығушылықтарына сәйкес білім беру қызметінің қосымша нысандарына бағыттау, баланың эмоционалды-мінез-құлық ерекшеліктерін жеке және топтық бейімдеу, әлеуметтенуді басқару және кеңес беру, түзету, тренинг түрінде баланың өзіне деген сенімін қалыптастыру.

Кибербуллинг кең етек жайған елдер Халықаралық сарапшылар кибербуллинг кеңінен етек жайған елдер рейтингінде Үндістан, Бразилия мен АҚШ-тың көш бастап тұрғанын айтады. Құрама Штаттарда онлайн әлімжеттік көрген балалардың 20 пайызы өзіне қол жұмсауды ойлайды екен. Мамандар балаларға кибербуллинг жасаудың негізгі себептерін былай көрсетеді. Интернеттегі әлімжеттікке не себеп? АҚШ-тағы балалардың 61 пайызы түріне байланысты онлайн кемістікке ұшырайды. 25 пайызы оқу үлгеріміне қатысты цифрлық әлімжеттік көреді. 17 пайызына шыққан тегін бетіне басады. Басқа себептерге сексуалды әлімжеттік, қаржылық жағдай және діни сенім жатады. Кибербуллинг себептері: Сырт келбеті 61% Оқу үлгірімі 25% Нәсілі 17% Сексуалды әлімжеттік 15% Қаржылық жағдайы 15% Діни наным-сенімі 11% Басқа себептер 20% Ересектер кибербуллингке ұшырайды Цифрлық әлімжеттіктен балалар ғана зардап шекпейді. Мұның зиянын үлкендер де тартып жүр. Әлемдегі ересектердің 40 пайызы кибербуллингке ұшырайды. Олардың

23 пайызының ұйқысы бұзылған. 49 пайызының кибербуллингке ұшырауына саяси көзқарасы себеп болған. Екінші орында сырт келбеті.

Қытайда кибербуллинг заңы қабылданды Әлемнің бірнеше елінде кибербуллингке қарсы заң қабылданған. Қытайда балаларға кибербуллинг жасауға тыйым салатын және алдын алатын заң биылғы жылдың 1 қаңтарында қабылданды. Құжат бойынша кінәлілерге 50 мың юаннан 500 мың юанға дейін айыппұл салынады. Бұл 3 миллион мен 30 миллион теңге аралығындағы сома. Кейінгі санақ бойынша, Қытайда интернет қолданушылар саны 1 миллиард адамнан асады. Оның 191 миллионы - балалар. Жапонияда кибербуллинг заңы қатайтылды Осындай заң жақында Жапонияда қабылданды. Күншығыс елінде интернет бетінде әлімжеттік жасағандар 1 жылға қамауға алынып, 300 мың иена айыппұл төлейді. Бұл шамамен 1 миллион теңге. Бұған дейін айыпты адам тек 30 күнге ғана қамалып, 10 мың иена, яғни 33 мың теңге төлеп құтылатын. Еуроодаққа кибербуллинг заңы керек Ирландияда 2018 жылы кибербуллингке ұшыраған Николь Фокс есімді жас қыз өзіне қол жұмсап, елде үлкен шу болды. Бойжеткеннің анасы 35 мың адамның қолын қойдырып, ақыры 2021 жылы арнайы заң қабылдатқан. Содан бері онлайн әлімжеттік жасағандар 5 жылға сотталып, 2 жарым мың еуроға дейін айыппұл төлейді. Бұл 1 миллион 230 мыңға жуық теңге.

Әлемде балалардың 30 пайызы кибербуллингтен зардап шегеді. Бұл кибербуллингті зерттеу жөніндегі ғаламдық орталықтың мәліметі. Ал ЮНЕСКО-ның дерегінше мүмкіндігі шектеулі оқушылардың 70 пайызы онлайн буллингке ұшырайды екен. Біріккен Ұлттар Ұйымы бұған ғаламдық деңгейде назар аудару керек деп отыр. Әлем елдері кибербуллингпен қалай күресіп жатыр. Шынында кибербуллинг – ғаламдық мәселе. Әсіресе жастар үшін қаупі зор. Біріккен Ұлттар Ұйымының тағы бір мәліметіне сүйенсек: әлем бойынша интернетті ең белсенді қолданушылар – 15 пен 24 жас аралығындағы жастар. Ақпарат және қоғамдық даму министрлігінің мәліметінше, өткен жылы ел аумағында кибербуллингке қатысы бар 10 мыңнан астам материалға шектеу қойылса, уәкілетті органның ұсынымдарымен интернеттегі 222 400-ден астам құқыққа қарсы материал жойылған. Ал бір тәулік ішінде әлеуметтік желілердегі контентті жоюды немесе бұғаттауды талап ететін заң Германия, Франция, Жаңа Зелландия, АҚШ секілді бірқатар дамыған елде қабылданған. Мәселен, АҚШ-тың 40-тан астам штатында кибербуллингке қолданылатын қылмыстық жаза өте қатаң. Сингапур, Оңтүстік Корея, Ресей мен Түркия мемлекеттері де осы әлеуметтік желі жөніндегі заңдарын қайта қарастырып, кибербуллингке қатысты жазаны күшейтіп жатыр.

Кибербуллинг онлайн қорқыту және қорлау үшін қылмыстық жауапкершілік мәселелерін жағдай жекелеген оң өзгерістерге қарамастан көптеген жағынан қанағаттанарлықсыз болып қала береді. Осылайша, құқық қорғау органдары тарапынан адам мен азаматтардың конституциялық құқықтар мен бостандықтарын тиімді қорғауды қамтамасыз етіп қана қоймай, азаматтардың құқықтарын жаппай және өрескел бұзу фактілеріне жол берген көптеген құқық бұзушылықтарды анықтап, олардың пайда болуына себептерді анықтап, профилактика жүргізу қажет. Мұндай жағдайды өзгерту қажеттілігі осы зерттеуді жүргізудің маңыздылығын көрсетеді.

Әдебиет

1. Gov.kz сайты // Интернет ресурс: https://www.gov.kz/situations/316/intro?lang=kk кіру уақыты 07.09. 2024

2. Welcome to the United Nations // Интернет ресурс: https://www.un.org/ru/ кіру уақыты 08.09.2024

3. Новости Zakon.kz // https://www.zakon.kz кіру уақыты 10.09.2024

СМАЙЛОВ Нуржигит Куралбаевич
профессор кафедры кибербезопасности и информационных технологий
Алматинской академии МВД Республики Казахстан им. М. Есбулатова, PhD

ОСНОВНЫЕ МЕТОДЫ И ПОДХОДЫ ДЛЯ РАСПОЗНАВАНИЯ РЕЧИ С ЦЕЛЬЮ ЗАЩИТЫ ОТ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Для борьбы с интернет-мошенничеством, связанным с распознаванием речи, используются различные методы и инструменты на основе искусственного интеллекта (ИИ). Эти технологии направлены на предотвращение мошеннических действий, таких как подделка голосов, мошенничество через телефонные звонки и фальсификация аудио. Ниже приведены основные методы и подходы, которые используются для распознавания речи с целью защиты от интернет-мошенничества.

1. Биометрия голоса

– *Speaker Verification* (Верификация диктора) – это процесс идентификации личности на основе её голосовых характеристик. Использование биометрии голоса позволяет защитить пользователей от подделки личности при помощи голосов, сгенерированных нейросетями.

Методы: Свёрточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), LSTM и трансформеры.

Инструменты: Nuance, Pindrop, VoiceVault.

2. Anti-Spoofing (Антиспуфинг) технологии

– *Антиспуфинг* – это технологии, разработанные для обнаружения мошеннических попыток подделки голоса или использования синтетических голосов для обмана систем распознавания речи.

Методы: Комбинация свёрточных нейронных сетей (CNN) и рекуррентных нейронных сетей (RNN), анализ акустических особенностей голоса (тембр, частота), спектральный анализ.

Примеры использования: Мошенники могут пытаться воспроизводить голос владельца банковского аккаунта, чтобы обмануть голосовую биометрическую систему. Антиспуфинг-системы выявляют, является ли голос подлинным или сгенерированным.

3. Нейросетевые модели для распознавания мошеннических вызовов

– Использование глубоких нейронных сетей (DNN) и сверточных нейронных сетей (CNN) для выявления мошеннических звонков на основе паттернов речи, лексики и других признаков.

– Примеры: Эти модели могут анализировать тон, темп и другие признаки, чтобы выявить аномальные или подозрительные звонки, исходящие от потенциальных мошенников.

4. Системы на основе поведенческих паттернов

– Анализ поведенческих характеристик речи может помочь выявить мошенничество. Например, мошенники часто используют определенные ключевые слова, фразы или агрессивный тон, чтобы манипулировать жертвами.

Методы: Использование моделей машинного обучения для анализа лексики, синтаксиса, интонации и эмоциональной окраски речи.

Примеры: Системы могут анализировать телефонные разговоры для определения мошеннических схем, таких как фишинговые звонки или социальная инженерия.

5. Технологии обработки естественного языка (NLP)

– Использование обработки естественного языка (NLP) для анализа содержания разговоров или аудиозаписей может помочь выявить подозрительную активность или мошенничество. NLP может выявлять подозрительные запросы, манипулятивные вопросы или необычные структуры речи, характерные для мошеннических звонков.

Методы: Языковые модели, такие как BERT, GPT, используются для анализа смысла и контекста фраз.

Примеры: Системы могут анализировать звонки для выявления попыток фишинга, предложений с обманом или манипуляций.

6. AI на основе анализа аномалий

– Анализ аномалий в голосовых данных может помочь выявить мошенничество. Системы ИИ анализируют нормальные паттерны взаимодействий и затем выявляют отклонения, которые могут свидетельствовать о мошенничестве.

Методы: Использование алгоритмов кластеризации и методов аномального анализа (например, Isolation Forest, One-Class SVM).

Примеры: Распознавание нестандартного поведения звонящих, таких как частые звонки с разными акцентами или странные голосовые паттерны, может указывать на мошенничество.

7. Технологии для выявления deepfake-голосов

– Распознавание синтетической речи и deepfake-голосов играет важную роль в защите от мошенников, использующих сгенерированные голоса для подделки личности.

Методы: Использование моделей нейросетей для анализа мелочей, таких как артефакты генерации голоса, отсутствие естественных интонационных колебаний или временных несоответствий.

Примеры: Anti-Deepfake системы могут защитить компании от мошенничества, где синтетический голос используется для подделки идентификации.

8. Системы для анализа эмоциональной окраски речи

– Определение эмоционального состояния звонящего на основе его голоса. Мошенники могут использовать агрессивные или чрезмерно дружелюбные тона, чтобы манипулировать жертвами.

Методы: Нейросети для анализа интонации, тембра и скорости речи.

Примеры: Эмоциональные изменения могут помочь системам выявить стресс или настойчивость, которые могут свидетельствовать о мошеннических намерениях.

9. Технологии анализа звуковой среды

– Мошенники часто используют фоновые шумы или изменяют окружающую среду, чтобы подделать звонки или запутать систему. AI-системы могут анализировать шумы, эхо и другие аспекты окружающей среды, чтобы выявить несоответствия.

Методы: Спектральный анализ, FFT (Fast Fourier Transform) для выявления аномалий в фоне разговора.

Примеры: Системы могут распознавать изменения в звуковой среде, характерные для подделки голосов.

10. End-to-End системы защиты

– Некоторые компании предлагают end-to-end решения, которые интегрируют различные методы ИИ для защиты от голосовых мошенничеств, включая анализ речи, поведенческих паттернов, аномалий и антиспуфинг.

Примеры: Pindrop, VoiceIt, Nuance предлагают решения, которые сочетают биометрию голоса и антиспуфинг для обнаружения мошенников.

11. Инструменты облачных сервисов

– Google Cloud Speech-to-Text, Amazon Transcribe, и Microsoft Azure Speech предлагают встроенные решения для анализа речи, которые могут быть адаптированы для обнаружения мошенничества. Они включают технологии для анализа контекста, эмоциональной окраски и аномалий.

Методы: Комбинация NLP, анализа голоса и методов машинного обучения для выявления подозрительных разговоров.

Эти методы помогают защититься от интернет-мошенничества, связанного с распознаванием и подделкой речи, а также повышают уровень безопасности в таких областях, как банковские услуги, голосовая аутентификация и взаимодействие с клиентами.

Распознавание речи является мощным инструментом в борьбе с интернет-мошенничеством. Используя различные методы и подходы, такие как автоматическое распознавание речи, анализ эмоций, биометрическая аутентификация и контекстный анализ, организации могут повысить свою защиту от мошеннических действий. Важно продолжать развивать эти технологии и адаптировать их к меняющимся условиям, чтобы эффективно противостоять угрозам и защищать пользователей.

КУБАНОВА Нургуль Байтоковна
Қазақстан Республикасының ІІМ М. Есболатов атындағы
Алматы академиясы киберқауіпсіздік және ақпараттық технологиялар
кафедрасының докторанты полиция майоры,

БЕЛГОЖАЕВА Лаззат Серикбаевна
Қазақстан Республикасының ІІМ М. Есболатов атындағы
Алматы академиясы иберқауіпсіздік және ақпараттық технологиялар
кафедрасының аға оқытушысы полиция подполковнигі

DDOS ШАБУЫЛДАРЫ ЖӘНЕ ИНТЕРНЕТТЕГІ АЛАЯҚТЫҚ: ҚАУІПТЕР МЕН ҚОРҒАНЫС ШАРАЛАРЫ

Ақпараттық жүйеге шабуыл – бұл ақпараттың үш қасиетінің бірін – қолжетімділік, тұтастық немесе құпиялылықты бұзуға бағытталған шабуылдаушының қасақана әрекеттерінің жиынтығы.

Шабуылды жүзеге асырудың үш кезеңі бар:

1. Шабуыл объектісі туралы ақпаратты дайындау және жинау кезеңі.
2. Шабуылдың жүзеге асу кезеңі.
3. Шабуылдаушы туралы іздерді және ақпаратты жою кезеңі.

Ақпараттық жүйеге шабуылдарды жіктеу бірнеше критерийлер бойынша жүзеге асырылуы мүмкін:

Оқиға орны бойынша:

Жергілікті шабуылдар (бұл түрдегі шабуылдың көзі жергілікті жүйенің пайдаланушылары және/немесе бағдарламалары болып табылады);

Қашықтағы шабуылдар (шабуыл көзі қашықтағы пайдаланушылар, қызметтер немесе қолданбалар болып табылады).

Ақпараттық жүйеге әсері бойынша:

Белсенді шабуылдар (нәтижесі ақпараттық жүйенің бұзылуы болып табылады);

Пассивті шабуылдар (ақпараттық жүйенің жұмысын бұзбай жүйеден ақпаратты алуға бағытталған).

Соңғы уақытта кәсіпорындар мен ұйымдардың ақпараттық жүйелеріне (АЖ) ену және олардың келтіретін зияны туралы жиі естиміз. Бұл кездейсоқ құбылыс емес, өйткені 21 ғасырдың ең маңызды парадигмаларының бірі барлық дерлік әкімшілік және өндірістік тізбектерді қамтитын инфокоммуникациялық технологиялар – әлеуетті зиянкестердің қызығушылығын арттыру. Бұл қызығушылықты АҚШ-тағы Карнеги университетінде ұйымдастырылған CERT зерттеу орталығының мәліметтері растайды. Осының барлығы ақпараттық ғасырға аяқ басқан бизнесмендерді кәсіпорынның қауіпсіздік деңгейін үнемі арттыру, ақпараттық шабуылдарға тиімді қарсы тұратын неғұрлым тиімді қорғау құралдарын енгізу қажеттілігі туралы ойлануға мәжбүр етеді.

Осыған байланысты, қазіргі уақытта ақпараттық ресурстарды қорғаудың негізгі құралдарының бірі ретінде компанияның құпияларын алғысы келетін бұзушылардың шабуылдарын уақтылы анықтауға және бұғаттауға мүмкіндік беретін шабуылдарды анықтау жүйелері (ШАЖ) бар екенін атап өткен жөн. Ақпараттық шабуылдарды анықтау әдістері туралы айтуды бастамас бұрын, бұзушының шабуылы не екенін анықтайық. Сонымен, шабуыл-бұл АЖ ақпараттық қауіпсіздігінің бұзылуына әкелетін бұзушының әрекеттерінің жиынтығы. Сәтті іске асырылған шабуыл нәтижесінде бұзушы, мысалы, АЖ-да сақталған ақпаратқа рұқсатсыз қол жеткізе алады, жүйенің жұмысын бұзады немесе АЖ деректерінің мазмұнын бұрмалайды. Шабуылдың ықтимал мақсаттары серверлер, пайдаланушылардың жұмыс станциялары немесе АЖ байланыс жабдықтары болуы мүмкін. Жалпы, кез-келген шабуылды төрт кезеңге бөлуге болады.

Сурет-1. Шабуылдың өмірлік циклы

DDoS-шабуыл (ағылш. Distributed Denial of Service – «қызмет көрсетуден бас тарту») – кең таралған және қауіпті желілік шабуылдардың бірі болып табылатын қызмет көрсетуден бас тарту түріндегі үлестірілген шабуыл. Шабуыл нәтижесінде заңды пайдаланушыларға, желілерге, жүйелер мен өзге де ресурстарға қызмет көрсету бұзылады немесе толық істен шығарылады. DDoS-шабуыл нәтижесінде сайтқа қызмет көрсететін серверлерге үлкен көлемдегі жалған сұратуларды өңдеуге тура келеді және сайт қарапайым пайдаланушы үшін қолжетімсіз болып қалады.

Мұндай шабуылдардан коммерциялық және ақпараттық сайттар зардап шегеді. Соңғы кезде хакерлер шабуылдардың мұндай түрін шабуылды тоқтату үшін ақша беруді талап ету мақсатындағы алаяқтық ретінде қолданады.

DDoS-шабуыл сызбалық түрде келесі көрініске ие: зардап шегуші ретінде таңдап алынған серверге әлемнің түрлі нүктелерінде орналасқан компьютерлерден көптеген жалған сұратулар келіп түседі. Нәтижесінде сервер өзінің бүкіл ресурстарын осы сұратуларды өңдеуге жұмсайды да, қарапайым пайдаланушылар үшін толық дерлік қолжетімсіз болып қалады. Жалған сұратулар жіберілген компьютерлердің пайдаланушылары өздерінің машиналарының хакерлер тарапынан қолданылғанын білмеуі де мүмкін. Осы компьютерлерде зиянкестер тарапынан орнатылған бағдарламалар «зомби» деп аталады. Компьютерлерді «зомбилендірудің» қорғалмаған желілерге рұқсатсыз кіруден троян-

бағдарламаларды қолдануға дейін баратын көптеген жолдары белгілі. Бұл дайындық кезеңі зиянкес үшін ең күрделі кезең болып табылады деуге болады.

DDoS түріндегі желілік шабуыл басқару орталығынан (зиянкестен) берілетін команда бойынша шабуылдауға ұшырайтын компьютерге оған заңды пайдаланушылардың қолжетімділігін тоқтатуға алып келетін ерекше сұратуларды жібере бастайтын ботнет (зомби-желі) – арнайы зиянкес бағдарламамен зарарланған үлкен көлемдегі компьютерлер көмегімен жүзеге асырылады. Бұл сызбаға қатысушылар саны өте көп болады: ботнетті әзірлеуге арналған бағдарламалық қамтамасыз етуді жазатындар, оны әзірлеуге тапсырыс беретіндер, зомби-желіге әкімгер болып, оны жалға беретіндер, шабуылға тапсырыс берушілер. Өкінішке орай, бүгінгі күні ботнеттермен күрес компьютерлерден зиянкес бағдарламалық қамтамасыз етуді жоюмен шектеліп отыр. Ботнет иелері мен оның «қызметтеріне» тапсырыс берушілер «кадр артында» қалады.

Ақпараттық қауіпсіздік мамандары DDoS-шабуылдардың келесі түрлерін бөліп қарастырады:

UDP flood – нысана-жүйе мекенжайына үлкен көлемдегі UDP (User Datagram Protocol) пакеттерді жолдайды. Бұл әдіс ең алғашқы шабуылдарда қолданылған болатын және қазіргі таңда ең зиянсыз шабуыл ретінде қарастырылады. Бас контроллер мен агенттер арасындағы алмасу барысында шифрленбеген TCP және UDP хаттамалары қолданылатындықтан, шабуылдың бұл түрін пайдаланатын бағдарламалар тез анықталады;

TCP flood – желілік ресурстарды «байлауға» алып келетін үлкен көлемдегі TCP-пакеттерді нысана мекенжайына жолдау;

TCP SYN flood – нәтижесінде жекелеген ашық қосылымдарды қадағалау үшін өзінің барлық ресурстарын жұмсауға тура келетін нысана-тораппен арадағы TCP-қосылымдарды анықтау үшін үлкен көлемдегі сұратуларды жолдау;

Smurf-шабуыл – пакеттерде осы сұратуды пайдаланатын бағытталған кең тарататын жіберілім мекенжайы бойынша ICMP (Internet Control Message Protocol) пинг-сұратулары, нәтижесінде дереккөздің жалған мекенжайы шабуыл нысанасына айналады;

ICMP flood – Smurf тектес, бірақ жіберілімдерсіз жүзеге асырылатын шабуыл.

Сипатталған шабуылдардың бірнеше түрін бірден қолданатын бағдарламалар ең қауіпті болып табылады. Олар TFN және TFN2K атауларына ие болды және хакерден жоғары деңгейдегі дайындықты талап етеді.

Сұратулар түрлі тараптардан келіп түсетіндіктен, шабуылдардың мұндай түріне тойтарыс беру біршама қиын болып табылады. Әдетте, қорғауға фильтрлеу мен блэкхолинг, сервер осалдықтарын жою, ресурстарды күшейту, бытыратып орналастыру (пайдаланушыларға қызмет көрсетуді жалғастыратын үлестірілген және көшірмесі бар жүйелерді қалыптастыру), бас тарту (шабуылдың нақты мақсатын басқа байланысы бар ресурстардан алу, IP-мекенжайды бүркемелеу) сияқты іс-шаралар жатады.

Егер Сіздің жеке серверлеріңіз бар болса, онда Сізге жасалатын шабуылды анықтауға арналған құралдарға ие болуыңыз қажет. DDoS-шабуыл нәтижесінде Сіздің сайтыңызға қолжетімділікпен байланысты туындаған мәселелерді неғұрлым ерте анықтасаңыз, оған тойтарыс беруге қажет шараларды соғұрлым ерте қолдана аласыз.

DDoS-ты кіріс трафигі профильдерінің механизмін жүзеге асыру көмегімен анықтауға болады. Егер серверіңіздегі трафиктің орташа есеппен санағандағы көлемі мен өзгеру динамикасын білсеңіз, оған тән емес өзгерістерді тез анықтау мүмкіндігі туады. DDoS-шабуылдардың басым бөлігі кіріс трафигі көлемінің шұғыл артуымен сипатталады және профильдер механизмі бұл секірудің шабуыл болып-болмағанын анықтауға көмектеседі.

Өткізу мүмкіндіктерінің есептері қосымша арналарды қосу керексіз екенін көрсетсе де, оларды қосу тиімді тәсіл болып табылады. Бұл жағдайда Сіз, мысалы, жарнамалық кампания, арнайы ұсыныстар немесе компанияңыздың БАҚ-та жарықтандырылуы нәтижесінде орын алуы мүмкін трафиктің күтпеген секірулерін еш зардапсыз билей аласыз.

DDoS-шабуылға тап болған жағдайда қолданылуы тиіс шаралар тізімі:

– шабуылдың орын алғанына көз жеткізіңіз. DNS-тің дұрыс емес конфигурациясын, маршрутизациямен байланысты мәселелерді және адами факторды қоса есептегенде, жұмыстағы іркілістің жалпы себептерін жойыңыз;

– техникалық мамандарға жүгініңіз. Техникалық мамандардың көмегімен шабуылға ұшыраған ресурстарды анықтаңыз;

– қосымшалардың маңыздылық басымдықтарын қалыптастырыңыз. Басымдыққа ие қосымшаларды сақтау үшін маңыздылық басымдықтарын қалыптастырыңыз. Интенсивті DDoS-шабуыл мен шектеулі ресурстар жағдайында негізгі пайда көздерін қамтамасыз ететін қосымшаларға баса назар аударыңыз;

– қашықтықтан қосылған пайдаланушыларды қорғаңыз. Ісіңіздің жұмысын қамтамасыз етіңіз: қолжетімділікке ие болуы тиіс қашықтықтағы сенімді пайдаланушылардың IP-мекенжайларын ақ тізімге енгізіп, бұл тізімді негізгі етіңіз. Бұл тізімді желіде таратып, оны қолжетімділік қызметін берушілерге жолдаңыз;

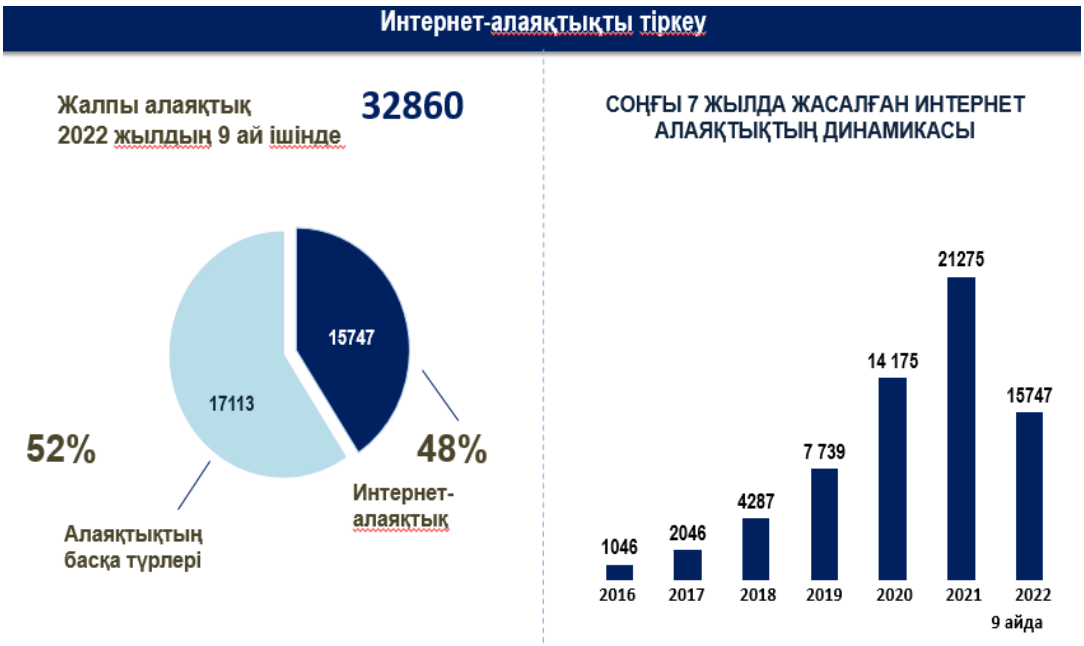
– шабуыл санатын анықтаңыз. Шабуылдың қандай түрімен бетпе-бет келдіңіз: Көлемді ме? Аз мөлшердегі әрі баяу ма? Сізге қызмет көрсетуші шабуылдың неғұрлым көлемді екенін хабарлайды;

– шабуыл дереккөздерінің мекенжайларымен күрес нұсқаларын анықтаңыз. Күрделі шабуылдар жағдайында Сізге қызмет көрсетуші дереккөздер санын анықтауда қиындыққа тап болады. Сіздің желіаралық экраныңыздағы шабуылдаушы IP-мекенжайлардың шағын тізімдерін оқшаулаңыз. Көлемді шабуылдарды геоорналасуы туралы деректер негізінде оқшаулауға болады;

– шабуылдарды қосымша деңгейінде оқшаулаңыз. Зиянкес трафикті анықтап, оның қандай құрал арқылы әзірленгенін анықтаңыз. Қосымша деңгейіндегі шабуылдардың белгілі бір бөлігін әрбір нақты жағдайда Сізде бар шешімдермен ұсынылатын контршаралардың көмегімен оқшаулауға болады;

– қоғаммен қарым-қатынасты басқарыңыз. Егер шабуыл жария болса, ресми хабарлама дайындап, қызметкерлеріңізді хабардар етіңіз. Егер салалық саясаттар мұны ескерсе, шабуылдың орын алу фактісін растаңыз. Егер ескермесе, техникалық қиындықтар бар екенін айтып, қызметкерлеріңізге сұрақ қойылған жағдайда, барлық сұрақтармен қоғаммен қарым-қатынас бөлімінің басшылығына жүгіну керек екенін айтыңыз.

Қазіргі кезде елімізде интернет алаяқтығының саны күрт өскен (сурет – 2).



Сурет – 2. Интернет алаяқтықты тіркеу

Интернеттің мүмкіндігін қылмыстық іс-әрекеттерін жүзеге асыру үшін оңтайлы пайдаланып жүрген алаяқтардың әдіс-тәсілдері күн сайын өзгеріп, жаңарып отырады. Уақыт талабынан олар да қалыс қалмай келеді. Әдетте алаяқтар әлеуметтік желілерге жалған интернет хабарландырулар орналастырады немесе аккаунт пен арнайы бет ашып, сайт жасап алады. Ең жиі кездесіп жүрген интернет алаяқтықтың түрлері: интернет арқылы сауда жасау және

қызмет көрсету, сондай-ақ өздерін банк қызметкері ретінде таныстырып, жеке деректерді иемдену және бөтен біреудің атынан онлайн-несие рәсімдеу арқылы жасалатын қылмыстар болып отыр. Интернет алаяқтық қазіргі қоғамның ең өзекті әрі маңызды мәселесіне айналды, қолында компьютер, смартфон, планшеті бар кез келген адамның кез келген уақытта ақпараттық жүйенің, соның ішінде интернет алаяқтардың құрбанына айналады.

Ақпараттық жүйені пайдаланып, алдау, арбау арқылы ақшалы болудың ең көп таралған жері – сауда-саттық маңы. Әсіресе сұранысқа ие Instagram әлеуметтік желісінде кімнің ақ, кімнің арам екенін ажырату өте қиын.

Ел көлемінде жүргізілетін Anti-fraud, Hi-tech жедел операцияларының барлығы кибер қылмыстардың алдын алу, осыған ұқсас заңсыздықтарды әшкерелеуге бағытталған. Әлеуметтік желілер мен мессенджерлерге, сондай-ақ ерекше қызығушылық танытатын пайдаланушылардың парақшаларына күн сайын мониторинг жүргізіледі. Бұл тәсіл интернеттегі алаяқтық схемаларды анықтауға көп септігін тигізеді.

Айта кетерлік тағы бір жайт, интернет алаяқтықтың көпшілігі трансшекаралық сипатқа ие. Мәселен, бір қылмыстық істе қаскүнем басқа өңірде, кейде тіпті басқа мемлекетте жүруі мүмкін. Сол себепті қылмыстың бұл түрін ашуға бірталай уақыт жұмсауға тура келеді. Өйткені өзге елде жүрген күдіктінің немесе жәбірленушінің жеке тұлғасы мен мекенжайын анықтау үшін шет мемлекеттегі құқық қорғау органдарына сұрау салу мен тапсырмалар жіберу міндетті болып саналады. Ал бұл іс-шараның барлығы бірден шешіле қоятын оңай шаруа емес.

Ақпараттық жүйеге басып кіруді анықтауға бола ма? Жауап: мүмкін. Алайда, бұл «мүмкін» АЖ ресурстарына ақпараттық шабуылдарды анықтау өте күрделі технологиялық процесс болып табылады, ол АЖ жұмыс істеу процесі туралы қажетті деректерді жинаумен, оларды талдаумен және ақырында шабуыл фактісін анықтаумен байланысты. Сондықтан шабуылды оның өмірлік циклінің барлық кезеңдерінде тиімді анықтау үшін мінез-құлық пен қолтаңба әдістерін біріктіріп қолдану қажет. Шабуылдарды анықтау проблемасына жоғарыда сипатталған кешенді тәсілді жүзеге асыру ғана компанияның ақпараттық жүйелеріне сәтті басып кіру қаупін едәуір азайтады және өндірістік және басқа құпиялардың жоғалуын болдырмайды, сонымен қатар 21 ғасыр – ақпарат ғасырындағы нарықта қол жеткізілген бәсекеге қабілеттілік деңгейін жоғалтуға жол бермейді.

Интернет алаяқтардан сақ болудың қарапайым қауіпсіздік шараларына тоқталатын болсақ, дербес деректерді, пластикалық карталардың мәліметтерін, кодтарды және құпия сөздерді ешкімге хабарламауға, белгісіз әрі тексерілмеген сайттар арқылы алдын ала төлем жүргізбеуге, күмәнді мәмілелер бойынша ақша аударымдарын жүзеге асырмауға, ұялы телефон мен компьютерге белгісіз қосымшаларды орнатпауға, кез келген сілтеме бойынша өтпеуге, спам хабарламаларға сенбеу керектігін айтып өтсек болады.

Әдебиет

1. Киберқауіпсіздік тұжырымдамасын («Қазақстан киберқалқаны») бекіту туралы. Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы №407 қаулысы.

2. 2014 жылы қабылданған және 2015 жылғы 1 қаңтардан бастап қолданыстағы Қазақстан Республикасының Қылмыстық кодексі.

3. Каиржанов С.Е. Криминологическая характеристика правонарушений связанных с нарушением работы информационных систем или информационно-коммуникационных сетей в Республике Казахстан // Криминологические и уголовно-правовые проблемы правонарушений в сфере защиты киберпространства в Республике Казахстан. – Алматы, 2018. – С. 78-83.

4. Ақпараттандыру туралы: Қазақстан Республикасының 2015 жылғы 24 қарашадағы №418-V Заңы, http:// www. zakon.kz.

5. Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы №832 қаулысы.

БЕЛГОЖАЕВА Лаззат Серикбаевна
Қазақстан Республикасының ІІМ М. Есболатов атындағы
Алматы академиясы киберқауіпсіздік және ақпараттық технологиялар
кафедрасының аға оқытушысы полиция подполковнигі

ИНТЕРНЕТТЕГІ АЛАЯҚТЫҚТЫ АНЫҚТАУДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТТІҢ МҮМКІНДІГІ

Интернеттегі алаяқтық – бүгінгі цифрлық дәуірде жиі кездесетін және күрделі мәселелердің бірі. Алаяқтар үнемі жаңа әдістер мен тәсілдерді қолдана отырып, желідегі пайдаланушыларды алдаудың жолдарын іздейді. Осыған орай, жасанды интеллект алаяқтықпен күресте маңызды құралға айналып отыр.

Жасанды интелект технологиялары деректерді талдау, үлгілерді анықтау және күмәнді әрекеттерді алдын ала болжау арқылы интернеттегі алаяқтықты тиімді түрде анықтай алады. Мысалы, алаяқтықпен күресу үшін нейрондық желілер мен машиналық оқыту алгоритмдерін қолдануға болады. Олар пайдаланушылардың мінез-құлық үлгілерін зерттеп, стандарттан ауытқуды жылдам табады, нәтижесінде күмәнді транзакциялар мен кіру әрекеттерін ерте анықтайды.

Сонымен қатар, жасанды интелект алаяқтықты анықтаудың автоматтандырылған жүйелерін құруға мүмкіндік береді. Бұл жүйелер миллиондаған дерек көздерін жылдам өңдеп, күдікті әрекеттерді дереу хабарлайды. Осылайша, жасанды интеллект көмегімен интернеттегі алаяқтықты тиімді басқаруға және пайдаланушылардың қауіпсіздігін арттыруға болады.

Жасанды интелектілердің интернеттегі алаяқтықты анықтаудағы басты артықшылықтарының бірі – оның үлкен көлемдегі деректерді қысқа мерзімде өңдеп, әртүрлі үлгілерді тез арада ажырату қабілеті. Кәдімгі әдістермен салыстырғанда, жасанды интеллект өзгерістерді жедел байқай алады, бұл алаяқтықтың алдын алу мүмкіндігін арттырады.

Бүгінде банктер, онлайн-сауда платформалары және әлеуметтік желілер жасанды интелектіні пайдалана отырып, күмәнді әрекеттерді бақылауда тиімділікке қол жеткізуде. Мысалы, онлайн транзакциялар кезінде жасанды интелект алгоритмдері әрбір операцияны бақылай отырып, алаяқтық белгілерін іздейді. Егер қандай да бір әрекет стандартты заңдылықтан тыс болып көрінсе, жүйе дереу ескерту жібереді немесе транзакцияны уақытша тоқтатады. Бұл әдіс клиенттердің жеке мәліметтерін қорғап, қаржылық шығындардың алдын алуға мүмкіндік береді.

Сонымен қатар, алаяқтар өз тәсілдерін үнемі жетілдіріп отырғандықтан, жасанды интелект жүйелері де үнемі жаңа деректермен оқытылып, жаңартылып отырады. Мұндай динамикалық процесс алаяқтықтың күрделене түсуіне қарамастан, онымен тиімді күресуді қамтамасыз етеді. Жасанды интелект арқылы интернеттегі қауіпсіздік жүйелерінің автоматтандырылуы адам қателіктерін азайтып, қолданушыларға сенімді қорғау береді.

Осылайша, жасанды интеллект интернеттегі алаяқтықты анықтауда маңызды рөл атқарады, әрі бұл технологияны жетілдіру арқылы онлайн қауіпсіздікті одан әрі нығайтуға болады. Жасанды интелект тек ағымдағы алаяқтықты анықтап қана қоймай, болашақта мүмкін болатын қауіптерді де болжап, алдын алуға қабілетті жүйелерді дамытуда шешуші құрал болып қала бермек.

Жасанды интеллекттің интернеттегі алаяқтықпен күрестегі тағы бір тиімділігі – деректерді өңдеу жылдамдығы мен ауқымдылығының арқасында кішігірім және байқалмайтын үлгілерді де анықтай алуы. Бұл, әсіресе, фишингтік шабуылдар, жалған аккаунттар, боттар арқылы жасалатын алаяқтық әрекеттер үшін өте маңызды. Жасанды интелект дәстүрлі әдістермен анықтау қиынға соғатын айлаларды да көріп, сол арқылы алаяқтықтың ерте кезеңінде анықтап, әрекет етуге мүмкіндік береді.

Бұған қоса, жасанды интеллекттің өздігінен үйрену қабілеті (machine learning) жүйелердің нақты уақыт режимінде жетілдірілуіне ықпал етеді. Яғни, бір рет тіркелген алаяқтық схемалары негізінде жасанды интелект жаңа әдістерді алдын ала тануға дағдыланады. Бұл жүйелерді тиімдірек әрі жылдам етеді, сондай-ақ адам араласуын азайтып, қауіпсіздіктің автоматтандырылуын жоғарылатады.

Болашақта интернеттегі алаяқтыққа қарсы тұруда жасанды интеллекттің рөлі арта түсетіні анық. Жасанды интеллектке негізделген жүйелердің дамуы арқылы интернет пайдаланушыларына сенімді қорғау мен қауіпсіздікті қамтамасыз етіп, онлайн алаяқтықтың алдын алу мүмкіндігі күшейе береді. Сол себепті компаниялар мен ұйымдар жасанды интелект технологияларын жетілдіріп, оларды кеңінен қолдануды басты назарда ұстауы керек.

Жасанды интеллекттің интернеттегі алаяқтықты анықтаудағы болашағы орасан зор. Әсіресе, жасанды интеллект технологиялары алдағы уақытта одан да күрделі және бейімделген алаяқтық схемаларын анықтауға қабілетті болады. Зерттеушілер тереңдетілген оқыту (deep learning) және табиғи тілді өңдеу (NLP) секілді әдістерді қолдана отырып, фишингтік электрондық хаттарды, жалған веб-сайттарды және жалған транзакцияларды нақты ажырататын жүйелерді дамытуды жалғастыруда. Бұл тәсілдер алаяқтардың алдау әрекеттерін анықтап қана қоймай, оларды дер кезінде тоқтата алады.

Сонымен қатар, алаяқтықпен күресу жүйелері мен жасанды интелект технологияларын біріктіру арқылы пайдаланушыларға алдын ала ескертулер жіберу, қауіп-қатерді болжау және онлайн-сервистерді нақты уақыт режимінде қорғау мүмкіндіктері кеңейеді. Бұл жүйелердің дамуымен бірге пайдаланушылардың жеке деректері мен қаржылық қауіпсіздігі нығая түседі.

Жасанды интеллектті алаяқтыққа қарсы күресте қолдану кең таралып келе жатқандықтан, оның тиімділігін арттыруға бағытталған зерттеулер де маңызды рөл атқарады. Әрбір жаңа жаңалық пен жетістік интернеттегі қауіпсіздікті жақсарта түсіп, жасанды интелектілердің алаяқтықпен күрестегі басты құралға айналуына ықпал етеді. Болашақта бұл технологиялар интернет пайдаланушылары үшін қауіпсіз және сенімді кеңістік қалыптастырады деп күтілуде.

Тағы бір маңызды мәселе – жасанды интелект жүйелерінің жұмысы үшін үлкен көлемде мәліметтер қажет. Бұл мәліметтерді жинау және сақтау кезінде деректердің құпиялылығы мен жеке мәліметтерді қорғау мәселелері туындауы мүмкін. Осыған орай, компаниялар жасанды интелект жүйелерін дамытқанда, пайдаланушылардың жеке ақпаратын қорғауды да басты назарда ұстауы қажет.

Сондай-ақ, жасанды интеллекттің дұрыс жұмыс істеуі үшін жоғары сапалы деректер керек. Егер деректер дұрыс өңделмесе немесе жеткілікті дәрежеде тазаланбаса, жасанды интелект жүйелері қате болжамдар жасап, жалған ескертулер жібере алады. Бұл жүйенің сенімділігіне кері әсер етуі мүмкін, сондықтан деректерді дұрыс өңдеу мен модельдерді үнемі тексеріп, реттеп отыру маңызды.

Жасанды интелект жүйелерінің тиімділігін арттыру үшін адам факторын толықтай жоққа шығаруға болмайды. Жасанды интеллект алаяқтықты анықтауда керемет құрал болға-

нымен, кейде адамның талдауы мен араласуы қажет болуы мүмкін. Сондықтан жасанды интелект пен адамның бірлесе жұмыс істеуі – интернеттегі алаяқтықпен күресудің ең тиімді тәсілдерінің бірі болып қала бермек.

Қорытындылай келе, жасанды интеллект интернеттегі алаяқтықты анықтау мен алдын алуда маңызды рөл атқаратыны сөзсіз. Оның деректерді өңдеу жылдамдығы, өздігінен үйрену мүмкіндігі және болжам жасау қабілеті алаяқтықпен күресте айтарлықтай көмегін тигізуде. Дегенмен, бұл технологияны дамыта отырып, оның шектеулерін ескеріп, жүйенің сенімділігі мен қауіпсіздігін қамтамасыз ету бағытында жұмыс істеу қажет. Жасанды интеллекттің жетілдірілуі интернет пайдаланушылары үшін қауіпсіздікті арттырып, онлайн кеңістікті сенімді етуге ықпал етеді.

Жасанды интеллекттің интернеттегі алаяқтықты анықтаудағы рөлін дамыту тек технологиялық жетістіктермен шектелмей, сонымен қатар құқықтық және этикалық мәселелерді де қамтиды. Жасанды интеллект жүйелерін қолдану барысында жеке деректердің құпиялылығы, пайдаланушылардың құқықтарын сақтау және деректерді әділетті пайдалану маңызды сұрақтарға айналады. Бұл салада нақты ережелер мен заңнамалар қабылданбаса, жеке ақпаратты теріс пайдалану, жеке өмірге қол сұғу қаупі арта түседі.

Сондықтан мемлекеттер мен реттеуші органдар жасанды интеллекттің интернеттегі алаяқтықпен күресудегі рөлін ескере отырып, заңдар мен реттеулерді әзірлеуі керек. Бұл ретте қолданушылардың деректерін жинау және пайдалану бойынша қатаң ережелерді енгізу, сондай-ақ жасанды интеллект жүйелерінің әділетті және транспарентті болуын қамтамасыз ету маңызды. Осының нәтижесінде интернеттегі қауіпсіздік пен алаяқтықпен күресу жүйелері теңдестірілген әрі заңды негізге сүйенген болмақ.

Этика мәселесіне қатысты тағы бір маңызды аспект – жасанды интеллекттің шешімдер қабылдаудағы бейтараптығы мен әділеттілігі. Жасанды интеллект алгоритмдерінің негізінде жатқан деректерде алдын ала жасырын немесе жанама түрде кездейсоқтықтар болуы мүмкін. Бұл кейбір топтарға қарсы дискриминация туындатуы мүмкін, сондықтан жүйелерді үнемі қадағалап, кемсітушілікті болдырмау үшін арнайы шаралар қабылдануы тиіс.

Жасанды интеллектің болашақтағы рөлі интернеттегі алаяқтықпен күресуден де асып, жалпы цифрлық қауіпсіздікті жақсартуға ықпал етеді. Қазіргі уақытта қолданылып жатқан технологиялар күмәнді транзакциялар мен жалған әрекеттерді анықтап қана қоймай, алдағы уақытта интернеттегі көптеген басқа қауіптерді де алдын ала болжай алатын жүйелерге айналуы мүмкін. Мысалы, жасанды интеллект кибершабуылдарды болжау және оларды алдын алу, цифрлық идентификацияның қауіпсіздігін қамтамасыз ету, сондай-ақ, жалпы интернет кеңістігіндегі қауіпсіздік шараларын жетілдіруде маңызды рөл атқаратыны айқын.

Қорытындылай келе, жасанды интеллекттің интернеттегі алаяқтықты анықтау мен оның алдын алудағы мүмкіндіктері кеңейіп келеді. Бұл технология цифрлық қауіпсіздікті қамтамасыз етудің маңызды құралына айналуда. Алайда, оның дамуы мен тиімділігі этикалық, құқықтық және деректерді қорғау саласындағы жауапты шешімдермен қатар жүруі тиіс. Жасанды интектілерді дұрыс бағытта дамыту арқылы интернеттегі алаяқтықты азайтып қана қоймай, жалпы онлайн кеңістікті қауіпсіз әрі сенімді етуге қол жеткізуге болады.

Әдебиет

1. Бородина Е.В., & Смагина О.А. (2018). «Методы машинного обучения для выявления финансового мошенничества.» *Вестник Санкт-Петербургского университета. Серия 10. Программирование*, 12(4), 217-229. https://doi.org/10.21638/spbu12.2018.403

2. Гусева Н.В., & Фролов И.А. (2019). «Использование искусственного интеллекта для обнаружения мошенничества в интернет-торговле.» *Информационные технологии и вычислительные системы*, 9(3), 25-34. https://doi.org/10.17213/itvs.2019.03.025

3. Кузнецова А.А. (2020). «Анализ и выявление финансовых мошенничеств с помощью методов машинного обучения.» *Финансовые исследования*, 15(1), 56-67. https://doi.org/10.2139/finres.2020.015

4. Соловьев С.П., & Петров И.В. (2021). «Алгоритмы машинного обучения для обнаружения мошенничества в банковских операциях» *Экономика и управление*, 16(4), 112-121. https://doi.org/10.33071/economy. 2021.04.112

5. Ильин Н.В., & Михайлова Е.А. (2022). «Методы искусственного интеллекта в борьбе с интернет-мошенничеством» *Вестник информационных технологий*, 6(2), 89-97. https://doi.org/10.31718/vit.2022.02.089

6. Михайлов В.П. (2020). «Анализ методов предсказательной аналитики в области финансового мошенничества.» *Финансовая аналитика*, 18(5), 110-119. https://doi.org/10.2139/finanal.2020.05.110

7. Тихомиров А.В., & Федоров С.А. (2021). «Искусственный интеллект в борьбе с киберугрозами.» *Кибербезопасность: проблемы и решения*, 7(3), 77-85. https://doi.org/10.24012/kibersb.2021.03.077

8. Шестаков А.Н., & Тихонов И.Р. (2023). «Методы анализа больших данных для обнаружения мошенничества.» *Современные технологии и инновации*, 12(1), 93-102. https://doi.org/10.31388/sti.2023.01.093

САВДАБАЕВ Ержан Сарсенович
преподаватель кафедры кибербезопасности и информационных технологий
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова старший лейтенант полиции

ИНСТРУМЕНТЫ ИИ ДЛЯ РАСПОЗНАВАНИЯ СИНТЕЗИРОВАННЫХ ГОЛОСОВ И ПОДДЕЛЬНЫХ ДОКУМЕНТОВ

С развитием технологий искусственного интеллекта (ИИ) появились мощные инструменты для создания поддельных голосов и документов, что открывает новые возможности для злоупотреблений. Эти технологии находят свое применение не только в развлекательных или коммерческих целях, но также используются киберпреступниками для мошенничества, кражи данных и дезинформации. В ответ на это стремительно развиваются системы ИИ, направленные на выявление и предотвращение фальсификаций. В данной статье мы рассмотрим ключевые инструменты и методы ИИ для распознавания синтезированных голосов и поддельных документов.

Опасности синтезированных голосов и поддельных документов

Синтезированные голоса и поддельные документы стали серьёзной угрозой в разных сферах. Мошенники могут использовать поддельные голоса для имитации звонков от представителей компаний или государственных учреждений, что увеличивает вероятность успеха фишинговых атак. Поддельные документы могут использоваться для создания фиктивных личностей, заключения фальшивых контрактов или выдачи себя за другого человека в юридических или финансовых вопросах. Совершенствование технологий генерации делает такие подделки всё более сложными для обнаружения невооруженным глазом или обычными методами проверки.

Примеры применения:

1. **Финансовые мошенничества**: Использование поддельных голосов для обмана банковских систем или служащих компаний.
2. **Подделка официальных документов**: Создание фальшивых договоров, паспортов или сертификатов для незаконных действий.
3. **Распределение фейковой информации**: Использование дипфейков для создания ложных новостей или искажения репутации.

Методы и инструменты распознавания синтезированных голосов

Технологии для распознавания синтезированных голосов быстро развиваются благодаря достижениям в области ИИ, машинного обучения и анализа звуковых сигналов. Рассмотрим основные подходы и инструменты, используемые для выявления фальшивых голосов.

1. Анализ звуковых характеристик

Одним из ключевых методов распознавания поддельных голосов является анализ звуковых характеристик, таких как тембр, интонация, паузы и изменения в громкости. Синтезированные голоса часто имеют неестественные тональные переходы и статичную интонацию, которые могут отличаться от голоса реального человека. Алгоритмы, обученные на настоящих записях голоса, могут обнаружить эти аномалии.

Инструменты:

– **Resemblyzer**: Это библиотека Python, которая анализирует звуковые записи и извлекает из них эмбеддинги голоса, что позволяет сравнивать и отличать поддельные и реальные голоса.

– **Adobe VoCo Detector**: Разработанное Adobe ПО, которое помогает выявить изменения в звуковых записях, создаваемых или модифицируемых с помощью ИИ.

2. Использование нейронных сетей

Нейронные сети и методы глубокого обучения играют важную роль в распознавании синтезированных голосов. Сверточные нейронные сети (CNN) могут анализировать звуковые спектрограммы, чтобы выявить отклонения в голосе, которые неуловимы для человеческого уха. Эти методы позволяют распознавать поддельные голоса на уровне микросекундных характеристик.

Пример:

DeepSonar – это инструмент, основанный на сверточных нейронных сетях, который может эффективно распознавать голоса, созданные с использованием алгоритмов глубокого обучения.

3. Анализ биометрических данных

Каждый человек имеет уникальные биометрические характеристики голоса, такие как частота, вибрации и продолжительность звука. Инструменты на основе ИИ могут сопоставлять биометрические параметры голоса с базой данных оригинальных записей, чтобы выявить фальсификации.

Пример:

– **Nuance Gatekeeper** – это система аутентификации, основанная на биометрии голоса, которая помогает выявлять подделки и защищать организации от использования синтезированных голосов.

4. Алгоритмы анализа речевого поведения

Еще один метод заключается в анализе паттернов речевого поведения. Люди, как правило, следуют определённым закономерностям в речи: темп речи, паузы, интонация. Синтезированные голоса часто создаются с минимальной проработкой таких деталей, что позволяет алгоритмам выявлять отклонения в речевых шаблонах.

Пример:

– **VoiceCatch** – система, которая отслеживает и анализирует изменения в темпе и ритме речи, помогая определить, был ли голос сгенерирован ИИ.

Методы и инструменты для распознавания поддельных документов

Поддельные документы могут быть созданы с использованием как традиционных методов подделки, так и современных технологий, таких как дипфейки или генеративные нейронные сети (GANs). Инструменты ИИ помогают автоматизировать процесс проверки подлинности документов.

1. Оптическое распознавание символов (OCR)

Одним из ключевых инструментов для анализа документов является технология **OCR (Optical Character Recognition)**. OCR позволяет автоматически извлекать текст из документов, проверять его на ошибки и сопоставлять с оригинальными шаблонами. Некоторые поддельные документы могут содержать неточности в тексте, которые выявляются с помощью алгоритмов машинного обучения.

Инструменты:

– **Tesseract OCR** – популярный open-source инструмент для извлечения текста, который можно использовать для анализа и проверки подлинности документов.

– **ABBYY FineReader** – мощный коммерческий инструмент для OCR и анализа документов с расширенными функциями проверки подлинности.

2. Анализ метаданных документа

Метаданные документа содержат информацию о его происхождении, авторе и дате создания. Алгоритмы ИИ могут анализировать метаданные для выявления несоответствий. Например, если документ был изменен после его создания, это может быть признаком подделки.

Инструменты:

– **ExifTool** – бесплатный инструмент для анализа метаданных, который позволяет выявлять изменения в документах и изображениях.

3. Сравнительный анализ изображений

ИИ-инструменты могут анализировать текстуры и элементы изображения документа для выявления фальсификаций. Например, с помощью нейросетей можно сравнить оригинальные и поддельные подписи, печати или водяные знаки, чтобы обнаружить любые отклонения от стандарта.

Инструменты:

– **Forensically** – онлайн-инструмент для анализа изображений, который помогает выявить манипуляции и изменения в изображениях, включая документы.

4. Анализ версионности и редактирования

Системы ИИ могут отслеживать историю редактирования документов, выявлять изменения, внесенные в файлы, и сравнивать их с оригинальной версией. Это особенно важно для юридических и финансовых документов, где любые изменения могут указывать на подделку.

Пример:

– **DocuSign** – платформа для электронных подписей, которая отслеживает каждый этап создания и изменения документа, что помогает предотвратить фальсификацию.

5. Использование генеративно-состязательных сетей (GANs)

Интересным и перспективным направлением является использование **генеративно-состязательных сетей (GANs)** не только для создания поддельных документов, но и для их распознавания. GAN-сети обучаются на больших объемах данных и могут выявлять тонкие различия между поддельными и оригинальными документами, которые невозможно обнаружить другими методами.

Пример:

DeepFake Text Detection – система, разработанная с использованием GAN, способная распознавать текстовые подделки, создаваемые с использованием алгоритмов генерации текста.

С развитием технологий генерации поддельных голосов и документов возрастают и риски, связанные с киберпреступностью и мошенничеством. Однако инструменты ИИ для их обнаружения также продолжают совершенствоваться, предлагая всё более точные и эффективные методы защиты. Использование нейронных сетей, анализа метаданных, биометрии голоса и текстового анализа позволяет вовремя выявлять фальшивки и предотвращать мошенничество. Важно продолжать развивать и внедрять эти технологии для обеспечения безопасности данных и сохранения доверия к цифровой информации.

САБИБОЛДА Акежан Муратулы
преподаватель кафедры кибербезопасности и информационных технологий
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова лейтенант полиции

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПО ГОЛОСУ: ТЕХНОЛОГИИ, ПРЕИМУЩЕСТВА

Биометрическая аутентификация по голосу – это процесс идентификации личности человека на основе его уникальных голосовых характеристик. С ростом киберугроз и мошенничества, эта технология становится всё более актуальной для обеспечения безопасности и защиты данных. В данной статье мы рассмотрим, как работает биометрическая аутентификация по голосу, её преимущества и потенциальные вызовы.

Принцип работы технологии

Биометрическая аутентификация по голосу основывается на анализе уникальных особенностей голоса человека. Каждое лицо имеет свои индивидуальные характеристики, такие как:

– **Частота и тональность**: Высота звука и тон, которые различаются у каждого человека.

– **Интонация и темп речи**: Способ, которым человек говорит, его ритм и скорость.

– **Артикуляция**: Манера произношения звуков и слов, включая акценты и диалекты.

Процесс аутентификации

1. **Запись голоса**: Пользователь произносит заранее заданную фразу или слово, что позволяет системе записать голосовую запись.
2. **Извлечение характеристик**: Система анализирует запись и извлекает биометрические данные, создавая уникальный голосовой шаблон.
3. **Сравнение**: При следующем обращении пользователя система сравнивает его текущий голос с ранее сохранённым шаблоном.
4. **Аутентификация**: Если данные совпадают, пользователю предоставляется доступ к защищённой системе или информации.

Преимущества биометрической аутентификации по голосу

1. Удобство использования

Биометрическая аутентификация по голосу не требует от пользователя запоминания паролей или ввода PIN-кодов. Достаточно произнести слово или фразу, что делает процесс аутентификации быстрым и простым.

2. Безопасность

Голосовые характеристики уникальны для каждого человека, что делает сложным их подделку. В отличие от паролей, которые могут быть украдены или угаданы, биометрические данные гораздо труднее скомпрометировать.

3. Дистанционная аутентификация

Технология позволяет аутентифицировать пользователей на расстоянии, что удобно для онлайн-сервисов, банковских приложений и клиентской поддержки.

4. Гибкость

Биометрическая аутентификация может быть интегрирована в различные устройства и системы, включая смартфоны, компьютеры и системы безопасности.

Вызовы и ограничения

1. Проблемы с точностью

Аутентификация по голосу может сталкиваться с проблемами точности в шумной обстановке или при наличии помех. Это может привести к ложным срабатываниям, как положительным, так и отрицательным.

2. Изменения в голосе

Факторы, такие как болезни, старение или эмоциональное состояние, могут повлиять на голос и затруднить аутентификацию. Необходимость учитывать эти изменения требует дополнительного обучения систем.

3. Уязвимость к подделкам

Несмотря на то что подделка голоса сложна, она возможна с использованием технологий синтеза речи. Это делает системы уязвимыми к мошенничеству.

4. Конфиденциальность и безопасность данных

Сбор и хранение биометрических данных поднимает вопросы о конфиденциальности и безопасности. Важно обеспечить защиту личной информации от несанкционированного доступа.

Применение биометрической аутентификации по голосу

1. Финансовые учреждения

Многие банки внедряют голосовую аутентификацию для улучшения безопасности клиентских операций. Это позволяет быстрее проверять личность клиентов при обращении в службу поддержки.

2. Государственные органы

Государственные учреждения используют биометрическую аутентификацию для управления доступом к чувствительной информации и услугам, таким как выдача документов или обработка заявлений.

3. Медицинские учреждения

Аутентификация по голосу может использоваться для защиты конфиденциальной медицинской информации и доступа к системам хранения данных.

Биометрическая аутентификация по голосу представляет собой мощный инструмент для повышения безопасности и удобства пользователей. Несмотря на свои преимущества, технология сталкивается с определёнными вызовами и ограничениями, которые необходимо учитывать при её внедрении. С учетом постоянного развития технологий и методов защиты данных, можно ожидать, что биометрическая аутентификация станет неотъемлемой частью системы безопасности в ближайшем будущем.

УРАЛОВА Фатима Сырлыбайкизи
преподаватель кафедры кибербезопасности и информационных технологий
Алматинской академии МВД Республики Казахстан
им. М. Есбулатова лейтенант полиции

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ВЫЯВЛЕНИИ ФАЛЬШИВЫХ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

Социальные сети стали неотъемлемой частью нашей жизни, позволяя пользователям общаться, делиться информацией и строить профессиональные и личные связи. Однако, наряду с ростом популярности социальных платформ, увеличивается и количество фальшивых аккаунтов, создаваемых для мошенничества, распространения фейковых новостей, киберпреступлений и манипуляций общественным мнением. В ответ на эту угрозу все больше компаний внедряют искусственный интеллект (ИИ) для выявления поддельных аккаунтов и защиты пользователей от возможных негативных последствий.

Фальшивые аккаунты в социальных сетях стали одной из самых острых проблем в современном цифровом мире. Они создаются злоумышленниками с различными целями, среди которых – кража данных, распространение спама и вредоносного ПО, а также манипуляции мнением пользователей. Эти поддельные профили представляют серьезную угрозу как для частных пользователей, так и для компаний и даже государственных структур. Чтобы лучше понять, почему создаются фальшивые аккаунты, стоит рассмотреть основные цели, которые преследуют мошенники.

Одной из ключевых причин создания фальшивых аккаунтов является распространение спама. Мошенники используют такие профили для массовой рассылки рекламных сообщений, зачастую с вредоносными ссылками, которые могут вести на фишинговые сайты. Эти сообщения могут быть нацелены как на конкретных пользователей, так и на случайные аккаунты в сети. Спам представляет собой не просто раздражающий фактор для пользователей, но и потенциальную угрозу безопасности, так как за безобидной рекламой может скрываться вредоносное ПО.

Второй по значимости целью является кража личных данных. Фальшивые аккаунты часто используются для фишинга – мошеннического метода получения конфиденциальной информации. Мошенники создают поддельные профили, имитируя известные бренды, сервисы или даже друзей пользователей, чтобы завоевать доверие и заставить пользователей раскрыть личные данные, такие как пароли или данные кредитных карт.

Организация кибератак также является одной из целей злоумышленников, использующих фальшивые аккаунты. Такие профили могут быть использованы для координации атак на системы компаний или государственных учреждений. Например, с помощью поддельных аккаунтов может быть инициирована атака типа «отказ в обслуживании» (DDoS), когда огромное количество запросов перегружает серверы и нарушает их работу.

Кроме того, фальшивые аккаунты играют ключевую роль в манипуляциях общественным мнением. Злоумышленники используют сотни и тысячи поддельных профилей для рас-

пространения ложной информации или продвижения определённых идей и взглядов. Фальшивые аккаунты могут имитировать общественное мнение, создавая иллюзию широкой поддержки определённых политических или социальных идей. Это особенно опасно в период выборов или общественных дебатов.

Последней, но не менее важной целью является мошенничество, при котором фальшивые аккаунты создаются с целью обмана пользователей. Злоумышленники притворяются доверенными лицами (друзьями, коллегами, родственниками), чтобы выманить деньги или другие ресурсы.

Таблица 1. Основные цели использования фальшивых аккаунтов

Цель Использования	**Описание**	**Примеры**
Распространение спама	Массовая рассылка рекламных, фишинговых или вредоносных сообщений пользователям, часто без согласия или с использованием вредоносных ссылок	Рассылка ссылок на фальшивые сайты, массовая реклама сомнительных товаров или услуг
Кража личных данных	Фальшивые профили используются для сбора личной информации, такой как контактные данные, пароли и данные кредитных карт, через фишинг или обман	Создание поддельных сайтов, которые имитируют реальные сервисы, для кражи паролей и данных банковских карт
Организация кибератак	Использование фальшивых аккаунтов для координации атак на сайты, рассылки вредоносного ПО или вирусов через ссылки или вложения	Координация атак типа DDoS, взлом корпоративных аккаунтов для дальнейшей рассылки вирусов
Манипуляции общественным мнением	Создание большого числа фальшивых аккаунтов для распространения фейковых новостей или продвижения определённых политических или социальных идей	Использование ботов для создания иллюзии общественной поддержки определённых идей, политических кампаний
Мошеннические схемы	Выманивание денег у доверчивых пользователей через ложные профили, притворяясь другом, родственником или другой доверенной персоной	Аферы с просьбами о финансовой помощи, фальшивые розыгрыши, обещания о «выигрышах» в конкурсах

Эта таблица демонстрирует основные цели, с которыми создаются фальшивые аккаунты, и даёт представление о тех угрозах, с которыми сталкиваются пользователи и организации. Каждая из целей может иметь значительные последствия, будь то финансовые потери, утечка данных или воздействие на общественное мнение. Понимание этих целей позволяет лучше оценить угрозу и разрабатывать эффективные методы противодействия, включая использование искусственного интеллекта.

Чтобы успешно противостоять растущей угрозе со стороны фальшивых аккаунтов, социальные сети всё чаще обращаются к технологиям искусственного интеллекта (ИИ). ИИ помогает автоматически обнаруживать подозрительные аккаунты, основываясь на их поведении, содержимом профилей и взаимодействиях с другими пользователями. Каждый метод ИИ играет свою уникальную роль в обеспечении безопасности пользователей и повышении доверия к платформам.

Таблица 2. Методы ИИ для выявления фальшивых аккаунтов

Метод ИИ	Применение	Описание примера применения
Анализ поведенческих данных	Отслеживание частоты публикаций, времени активности, взаимодействий с другими аккаунтами, чтобы выявить подозрительное поведение	Например, если аккаунт делает 100 публикаций в минуту или добавляет в друзья 1000 пользователей за день – это сигнал
Обработка естественного языка (NLP)	Анализ текстов для выявления шаблонов, характерных для фальшивых аккаунтов, таких как спам или повторяющиеся фразы	Анализ комментариев на наличие повторяющегося контента, фраз-спамеров, или «стоп-слов», которые указывают на фейк
Анализ изображений	ИИ анализирует фотографии профилей, выявляя дубликаты, низкокачественные изображения или неестественно обработанные фото	Обнаружение использования одной и той же фотографии в сотнях профилей или анализ на присутствие манипуляций с изображением
Графовый анализ связей	Изучение структуры связей аккаунтов, чтобы выявить неестественные или подозрительные сети взаимодействий	Если один аккаунт связан с множеством новых, подозрительных профилей, это может говорить о том, что аккаунт фальшивый

Эта таблица описывает различные методы ИИ, которые применяются для выявления фальшивых аккаунтов. Эти технологии позволяют анализировать поведение пользователей, структуру их социальных связей, содержание текстов и изображений. Благодаря применению ИИ, социальные сети могут эффективно блокировать поддельные аккаунты до того, как они успеют причинить вред.

3 таблица демонстрирует, насколько масштабной является проблема фальшивых аккаунтов и как активно социальные сети работают над их выявлением и блокировкой с помощью технологий ИИ.

Таблица 3. Количество заблокированных фальшивых аккаунтов (2023 г.)

Социальная сеть	Заблокировано аккаунтов	Доля от общего числа пользователей (%)	Применение ИИ
Facebook	2.7 миллиарда	12%	Facebook применяет машинное обучение для анализа активности пользователей и их взаимодействий с контентом.
Instagram	1.1 миллиарда	10%	Instagram использует ИИ для анализа фотографий, комментариев и данных взаимодействий для блокировки фальшивых аккаунтов.
Twitter	500 миллионов	15%	Twitter анализирует социальные графы и поведение аккаунтов для выявления и блокировки ботов и поддельных профилей.

Количество заблокированных фальшивых аккаунтов в 2023 году поражает: Facebook, Instagram и Twitter активно работают над улучшением своих алгоритмов ИИ для выявления и предотвращения угроз. Эти данные подчеркивают, насколько значительна проблема фальшивых аккаунтов и почему необходимо продолжать развивать ИИ-технологии для обеспечения безопасности пользователей.

Таким образом, каждая таблица в статье не только иллюстрирует ключевые аспекты проблемы фальшивых аккаунтов, но и подчёркивает важность использования современных технологий, таких как искусственный интеллект, для борьбы с этой угрозой. Первая таблица помогает наглядно представить основные цели, которые преследуют злоумышленники, создавая поддельные профили, и показать разнообразие угроз – от кражи данных до манипуляций общественным мнением. Вторая таблица раскрывает передовые методы, которые применяются ИИ для выявления фальшивых аккаунтов, демонстрируя, как технологии анализируют поведение пользователей, их текстовые взаимодействия и изображения для определения подозрительных активностей. Наконец, третья таблица показывает масштабы проблемы, представляя статистику по блокировке фальшивых аккаунтов крупнейшими социальными сетями.

Эти данные подчеркивают, что применение ИИ – это не просто современный тренд, а необходимость для защиты цифровых платформ. С ростом сложности мошеннических схем, развитие и совершенствование технологий ИИ будет играть всё более значимую роль в обеспечении безопасности пользователей и поддержании доверия к социальным сетям.

Использование фальшивых аккаунтов в социальных сетях является серьёзной угрозой для пользователей и компаний по всему миру. Мошенники создают поддельные профили с различными целями, от кражи личных данных и распространения спама до манипуляций общественным мнением и организации кибератак. Эти аккаунты наносят значительный ущерб как отдельным пользователям, так и всей экосистеме социальных сетей, подрывая доверие к онлайн-платформам.

Однако, с развитием технологий искусственного интеллекта, социальные сети всё активнее внедряют инновационные решения для выявления и блокировки таких аккаунтов. Методы ИИ, такие как анализ поведенческих данных, обработка естественного языка (NLP), анализ изображений и графовый анализ связей, позволяют выявлять фальшивые аккаунты с высокой точностью и минимальными затратами времени. Эти технологии становятся мощным инструментом в борьбе с мошенничеством и киберугрозами.

Статистические данные показывают, что социальные сети активно борются с проблемой – миллиарды фальшивых аккаунтов уже заблокированы, и эта цифра продолжает расти. Однако с учётом того, что мошенники также используют ИИ для создания более правдоподобных профилей, вызовы остаются. Для эффективной борьбы с фальшивыми аккаунтами необходимо не только совершенствовать технологии ИИ, но и усиливать межплатформенное сотрудничество и обмен информацией о киберугрозах.

В будущем роль искусственного интеллекта в обеспечении безопасности социальных сетей будет только возрастать, помогая справляться с новыми угрозами и защищать цифровое пространство от злоумышленников.

Литература

1. Агроскин Д.В. (2021). Информационная безопасность в социальных сетях: методы и инструменты защиты. – М.: Наука.
2. Иванов А.А., & Петров Б.В. (2022). Применение искусственного интеллекта в борьбе с интернет-мошенничеством. Журнал информационных технологий и безопасности, 45(3), 56-72.
3. Джонс Т., & Уильямс К. (2020). AI and Social Media: Fighting Fake Accounts with Machine Learning. Cambridge: Academic Press.
4. Фейсбук. (2023). Отчёт о прозрачности за 2023 год. Получено с https://transparency.facebook.com
5. Ким М.Т., & Хуанг П.Л. (2019). Deep Learning Techniques for Detecting Fake Accounts in Social Media Platforms. Cybersecurity and Data Science Review, 34(2), 102-120.
6. Ли С.Я., & Чжоу Х.К. (2021). Анализ графов для выявления ботов в социальных сетях. Журнал прикладных технологий искусственного интеллекта, 23(4), 88-105.
7. Twitter. (2023). Transparency Report: Fake Account Detection and Removal. Retrieved from https://transparency.twitter.com
8. Петров И.А., & Сидоров В.И. (2023). Обзор методов защиты от фальшивых аккаунтов с применением искусственного интеллекта. Кибербезопасность в цифровую эпоху, 6(1), 43-59.
9. Smith, J., & Johnson, R. (2023). Machine Learning for Spam Detection in Social Media. International Journal of Cybersecurity and Artificial Intelligence, 29(1), 114-130.
10. Instagram. (2023). Отчёт по борьбе с фальшивыми аккаунтами. Доступно на https://help.instagram.com

РАМАЗАНОВА Жаннұр Ерқаликызы
магистрант 2 курса Satbayev University

ИМЕНАЛИНОВА Асел Тлегеновна
магистрант 2 курса Satbayev University

РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВУЗА

В современном информационном обществе защита данных и конфиденциальности стала одной из основных задач для любой организации, включая высшие учебные заведения. ВУЗы хранят большое количество личной информации о своих студентах, преподавателях и сотрудниках, а также проводят множество операций, связанных с финансами и академическими данными. Поэтому разработка защищенной системы аутентификации является необходимостью для обеспечения безопасности информационной системы ВУЗа.

Однако традиционные методы аутентификации, такие как пароли или PIN-коды, все чаще подвергаются атакам со стороны злоумышленников. В результате этого возникает риск несанкционированного доступа к системе и утечки конфиденциальных данных. Для борьбы с этими угрозами требуется использование новых технологий и методов аутентификации, которые будут эффективно защищать информацию ВУЗа от несанкционированного доступа.

Цель данной статьи состоит в изучении проблематики разработки защищенной системы аутентификации для информационной системы ВУЗа. Будут рассмотрены основные методы и инструменты, используемые при создании такой системы, а также предложены рекомендации по ее эффективному внедрению. При этом будет уделено внимание как техническим аспектам разработки системы, так и организационным мерам по обеспечению безопасности данных. Результатом работы должна быть надежная и устойчивая к взлому система аутентификации, способная эффективно защитить информацию ВУЗа от потенциальных угроз.

Актуальность проблемы защиты информации в ВУЗах. Актуальность проблемы защиты информации в ВУЗах состоит в том, что университетские информационные системы содержат большое количество конфиденциальных данных, которые требуют надежной защиты. В последние годы наблюдается увеличение числа кибератак на информационные системы ВУЗов, что может привести к несанкционированному доступу к конфиденциальным данным студентов, преподавателей и сотрудников. Кроме того, ВУЗы активно привлекают новые информационные технологии, такие как электронное обучение и удаленная работа, что еще больше усиливает необходимость защитить информацию от киберугроз.

Несмотря на существующие методы и средства защиты информации, ВУЗы всё еще испытывают проблемы с аутентификацией пользователей и обеспечением безопасности их идентификационных данных. Традиционные методы аутентификации, такие как пароли, могут быть легко подобраны или похищены злоумышленниками, поэтому требуется разработка более надежных и защищенных методов.

Защищенная система аутентификации для информационной системы ВУЗа имеет целью надежно и безопасно определить легитимность доступа к системе, а также защитить личные данные пользователей от несанкционированного доступа. Она должна предоставлять возможность аутентификации посредством не только паролей, но и других биометрических данных, таких как отпечатки пальцев, голос и лица.

Разработка такой системы требует учета особенностей информационной системы ВУЗа и ее пользователей. Необходимо учитывать большое количество пользователей, различные роли и уровни доступа, а также потребности в масштабируемости и производительности. Кроме того, разработка должна быть совместима с существующими системами и позволять удобное управление правами доступа.

В современном мире разработка безопасной системы аутентификации становится все более важной задачей. Информационные системы ВУЗов не являются исключением, и требуют надежной защиты информации и пользователей. Разработка защищенной системы аутентификации для ВУЗов – это неотъемлемая часть усовершенствования информационной безопасности в ВУЗах и обеспечение конфиденциальности и защиты данных всех участников образовательного процесса.

Анализ существующих систем аутентификации в информационных системах ВУЗов. Аутентификация в информационных системах вузов - это процесс проверки подлинности пользователей и разрешения доступа к системе. В современном высшем образовании информационные системы широко используются для управления учебным процессом, учета успеваемости студентов, регистрации и оплаты курсов, а также для хранения и обработки персональных данных студентов и сотрудников. Поэтому безопасность и эффективность системы аутентификации вуза являются критическими аспектами.

Одной из наиболее распространенных систем аутентификации, используемых в информационных системах вузов, является система «логин/пароль». Пользователь вводит свой логин и пароль, которые затем проверяются на соответствие данным в базе данных. При этом многие вузы требуют от студентов и сотрудников смены пароля через определенный период времени для повышения безопасности. Однако такая система имеет недостатки, такие как возможность подбора пароля, утечка пароля в случае скомпрометирования базы данных и необходимость запоминания множества паролей для доступа к различным системам.

Более совершенной системой аутентификации является двухфакторная аутентификация, которая требует от пользователя предоставить два различных фактора для подтверждения своей подлинности. Например, система может потребовать ввода логина и пароля, а затем отправить одноразовый секретный код на зарегистрированный телефон пользователя. Такая система обеспечивает более высокий уровень безопасности, так как даже в случае компрометации пароля злоумышленникам будет сложно получить доступ к системе без физического доступа к телефону пользователя.

Также существует система аутентификации на основе биометрических данных, которая использует уникальные физические характеристики пользователя, такие как отпечатки пальцев, голос или сетчатка глаза для проверки подлинности. Это обеспечивает высокий уровень безопасности, так как биометрические данные сложно подделать или украсть. Однако такая система требует наличия специального оборудования, что может быть дорого и неудобно для пользователя.

В итоге, анализ существующих систем аутентификации в информационных системах вузов показывает, что не существует универсального решения, подходящего для всех вузов. Каждый вуз должен анализировать свои потребности и на основе этого выбирать наиболее подходящую систему аутентификации. Следует учитывать уровень безопасности, удобство использования, стоимость внедрения и поддержки, а также соответствие системы требованиям законодательства о защите персональных данных. Разработка защищенной системы

аутентификации для информационной системы вуза - это трудоемкий и ответственный процесс, но он необходим для обеспечения безопасности и защиты данных вуза.

Проектирование и разработка защищенной системы аутентификации для ВУЗа. Для обеспечения безопасности информационной системы (ИС) вуза крайне важно разработать и реализовать надежную систему аутентификации, которая позволит только авторизованным пользователям получить доступ к системе.

Первый шаг в проектировании системы аутентификации - определение требований и функциональности. В данном случае, наша система должна обеспечивать безопасный и удобный доступ для различных пользователей, таких как студенты, преподаватели и администраторы. Также важно предусмотреть возможность масштабирования системы и поддержку различных методов аутентификации, таких как пароль, двухфакторная аутентификация или биометрическое распознавание.

После определения требований, следует разработка архитектуры системы. Вероятно, наша система будет состоять из нескольких компонентов, например, клиентского приложения, сервера аутентификации и базы данных пользователей. Важно обеспечить безопасность передачи данных между клиентом и сервером, например, с использованием протокола HTTPS. Кроме того, необходимо учесть возможность распределения нагрузки и отказоустойчивость системы.

Следующий этап – разработка пользовательского интерфейса. Важно, чтобы интерфейс был интуитивно понятным и удобным для всех категорий пользователей. Например, можно предусмотреть возможность выбора метода аутентификации, а также предоставить возможность сменить пароль или просмотреть историю входов.

После этого следует разработка и реализация механизма аутентификации. В зависимости от выбранного метода, это может быть разработка алгоритмов для проверки пароля или реализация биометрического распознавания. Важно учесть потенциальные уязвимости и применить соответствующие меры защиты, такие как хэширование паролей либо использование криптографических протоколов.

Кроме того, необходимо разработать механизм системного журналирования, который позволит фиксировать все попытки входа, а также ошибочные или подозрительные действия пользователей. Это позволит быстро реагировать на любые потенциальные угрозы безопасности и предпринимать соответствующие меры.

Важно также учесть аспекты управления доступом. Например, предусмотреть возможность установки различных уровней доступа для различных категорий пользователей и ограничения доступа к определенным разделам или функциям системы. Это позволит обеспечить не только безопасность данных, но и конфиденциальность.

В заключение, разработка защищенной системы аутентификации для информационной системы ВУЗа требует тщательного планирования и проектирования, учета различных требований и функциональности, а также применения современных методов безопасности. Только такая система сможет надежно защитить конфиденциальность и целостность данных, а также обеспечить безопасный доступ различных категорий пользователей. Разработка и реализация системы аутентификации для информационной системы вуза не является одноразовым процессом. Система должна быть подвергнута регулярной периодической проверке и обновлению, чтобы обеспечить непрерывную защиту ИС от новых угроз и уязвимостей.

Оценка эффективности и безопасности разработанной системы аутентификации в ВУЗе. Для обеспечения безопасности информационных систем вузов необходимо разработать эффективные и надежные системы аутентификации. Оценка эффективности и безопасности такой системы играет важную роль в обеспечении защиты данных и конфиденциальности пользователей.

Первым шагом при оценке эффективности и безопасности системы аутентификации является анализ ее функциональности. Важно определить, какие возможности предоставляет система и как она решает задачи аутентификации. Для этого проводятся испытания и тестирование системы на различных уровнях нагрузки. Проводятся симуляции атак и попыток несанкционированного доступа к системе, чтобы проверить ее защитные механизмы и эффективность работы в реальном времени.

Кроме того, оценка безопасности системы включает анализ уязвимостей и рисков. Идентифицируются уязвимые места в системе, которые могут стать целью злоумышленников. Производится анализ возможных угроз и рисков, связанных с использованием системы аутентификации. На основе найденных уязвимостей и рисков разрабатываются меры по их устранению и минимизации.

Важным аспектом оценки эффективности и безопасности системы аутентификации является анализ производительности. Проверяется, насколько быстро и эффективно происходит процесс аутентификации пользователей. Определяются показатели производительности, такие как время отклика системы, количество одновременных аутентификаций и другие.

Для проведения оценки эффективности и безопасности системы аутентификации необходимо также провести оценку пользовательского опыта. Исследуется удобство использования системы, ее понятность и интуитивность интерфейса. Оцениваются возможности пользователя взаимодействовать с системой, а также наличие дополнительных функций, таких как восстановление пароля или подтверждение идентичности пользователя.

Выводы, полученные в результате оценки эффективности и безопасности системы аутентификации, позволяют определить ее готовность к использованию в информационной системе вуза. Если система успешно прошла испытания и достаточно надежна для обеспечения безопасности данных, она может быть внедрена в ВУЗ. Однако, если обнаружены серьезные проблемы или уязвимости, необходимо провести доработку системы или выбрать другое решение для обеспечения безопасности информационных ресурсов ВУЗа.

Оценка эффективности и безопасности разработанной системы аутентификации для информационной системы вуза является важным этапом в обеспечении защиты данных и конфиденциальности пользователей. Правильно проведенная оценка позволяет выявить возможные проблемы и уязвимости, а также разработать меры по их устранению. Результаты оценки помогут определить готовность системы к использованию и обеспечить эффективную защиту информационных ресурсов ВУЗа.

Литература

1. Отчёт об утечках конфиденциальной информации в 2015 году. Предварительные итоги [Электронный ресурс] // Zecurion Analytics: сайт. – URL: https://www.zecurion.ru/upload/iblock/1e5/Zecurion Data Leaks 2016 full.pdf (дата обращения: 27.03.2019).

2. Time-based One-time Password Algorithm [Электронный ресурс] // Википедия - свободная энциклопедия: сайт. – URL: http://ru.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm (дата обращения: 03.04.2019)

3. Persson, O., & Wermelin, E. (2017). A Theoretical Proposal of Two-Factor Authentication in Smartphones.

4. Song, R. (2010). Advanced smart card based password authentication protocol. Computer Standards & Interfaces, 32 (5-6), 321-325.

5. Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. Journal of Intelligent Manufacturing, 25 (2), 217-230.

«Интернеттегі алаяқтықты анықтау үшін жасанды интеллект мүмкіндіктерін пайдалану» тақырыбындағы дөңгелек үстел
ҚАРАРЫ

Дөңгелек үстелге академияның профессорлық-оқытушылық құрамы, жоғары оқу орнынан кейінгі білім беру факультетінің тыңдаушылары, сонымен қатар IT компаниялардың ақпараттық қауіпсіздік мамандары қатысты.

Қатысушылардың баяндамалары біршама ғылыми қызығушылық тудырды. Біз бірге келесі қорытындыға келдік:

– Фишинг, жеке мәліметтерді ұрлау, қаржылық алаяқтық және криптовалютамен айлашарғы жасау сияқты онлайн алаяқтық жеке және корпоративтік қауіпсіздікке қауіп төндіре отырып, барған сайын күрделі және күрделі болып барады.

– Жасанды интеллект және машиналық оқыту аномальды әрекеттерді анықтау, үлкен деректерді талдау және қауіпті болжау жүйелерін жасау үшін бірегей мүмкіндіктерді қамтамасыз етеді.

– Қазіргі заманғы AI әдістері, соның ішінде нейрондық желілер, машиналық оқыту алгоритмдері және нақты уақыттағы деректерді талдау киберқауіпсіздік саласында өзінің тиімділігін көрсетті, бірақ одан әрі дамыту мен жетілдіруді қажет етеді.

– Пайдаланушы әрекетін талдауға арналған AI шешімдерін әзірлеу – өткен деректер негізінде алаяқтық әрекеттерді болжауға және алдын алуға, транзакциялар мен пайдаланушы әрекеттеріндегі күдікті үлгілерді анықтауға қабілетті жүйелерді жасау үшін машиналық оқыту мен мінез-құлық талдауын пайдалану.

– Жасанды интеллектті қолданыстағы қауіпсіздік жүйелеріне біріктіру – антивирустық бағдарламалар, желіаралық қалқандар және шабуылдың алдын алу жүйелері сияқты бар киберқауіптерден қорғау құралдарымен біріктіре алатын AI технологияларын дамыту. Бұл интернет-алаяқтықтан неғұрлым толық қорғауды қамтамасыз етеді.

– АТ-қауіпсіздік мамандарын даярлау және олардың біліктілігін арттыру – киберқауіпсіздік саласында АИ жүйелерімен жұмыс істейтін мамандарды оқыту және біліктілігін арттыру бағдарламаларын әзірлеу. Бұл интернет-алаяқтықпен күресте жаңа құралдарды тиімді пайдалануға мүмкіндік береді.

– Мемлекеттік, жеке және халықаралық ұйымдар арасындағы ынтымақтастық және деректер алмасу – алаяқтықпен күресудің жаңа қауіптері мен әдістері туралы ақпарат алмасу үшін мемлекеттік органдар, жеке компаниялар және халықаралық ұйымдар арасында ынтымақтастық орнату. Бірге жұмыс істеу сізге жаңа қиындықтарға тезірек және тиімдірек жауап беруге мүмкіндік береді.

– Киберқауіпсіздік саласында АИ қолдану стандарттарын құру – пайдаланушы деректерін қорғау және этикалық нормаларды сақтауды қоса алғанда, интернет-алаяқтықтан қорғау контекстінде АИ-ді пайдалануды реттейтін халықаралық стандарттар мен ережелерді әзірлеу және енгізу.

– Жасанды интеллектті пайдаланудағы этика және жауапкершілік – құпиялылықты бұзу, қателерді қате анықтау және жеке өмірге шамадан тыс қол сұғу сияқты ықтимал келеңсіз салдарды болдырмау үшін Интернеттегі алаяқтықпен күресуде AI пайдалануды реттейтін зерттеулер жүргізу және этикалық стандарттарды әзірлеу.

РЕЗОЛЮЦИЯ
круглого стола на тему «Использование возможностей искусственного интелекта для выявления интернет-мошеничеств»

В работе круглого стола приняли участие профессорско-преподавательский состав, слушатели факультета послевузовского образования нашего ВУЗа, а также специалисты IT-компании по информационной безопасности.

Определенный научный интерес вызвали доклады участников. Сообща мы пришли к следующим выводам:

– Интернет-мошенничества, такие как фишинг, кража личных данных, финансовые махинации, а также манипуляции с криптовалютами, становятся всё более сложными и изощрёнными, создавая угрозы для личной и корпоративной безопасности.

– Искусственный интеллект и машинное обучение предоставляют уникальные возможности для обнаружения аномальных действий, анализа больших данных и создания систем предсказания угроз.

– Современные методы ИИ, включая нейронные сети, алгоритмы машинного обучения и анализ данных в реальном времени, уже продемонстрировали свою эффективность в области кибербезопасности, но требуют дальнейшей разработки и совершенствования.

– Развитие ИИ-решений для анализа поведения пользователей – использование машинного обучения и анализа поведения для создания систем, которые способны на основе прошлых данных предсказывать и предотвращать мошеннические действия, выявлять подозрительные паттерны в транзакциях и действиях пользователей.

– Интеграция ИИ в существующие системы безопасности – развитие технологий ИИ, способных интегрироваться с уже существующими средствами защиты от киберугроз, такими как антивирусные программы, фаерволы и системы предотвращения вторжений. Это обеспечит более комплексную защиту от интернет-мошенничеств.

– Обучение и повышение квалификации специалистов по ИТ-безопасности – развитие программ обучения и повышения квалификации для специалистов, которые будут работать с ИИ-системами в сфере кибербезопасности. Это позволит эффективно использовать новые инструменты в борьбе с интернет-мошенничествами.

– Сотрудничество и обмен данными между государственными, частными и международными организациями – установление сотрудничества между правительственными структурами, частными компаниями и международными организациями для обмена информацией о новых угрозах и методах борьбы с мошенничествами. Совместная работа позволит быстрее и эффективнее реагировать на новые вызовы.

– Создание стандартов для применения ИИ в области кибербезопасности – разработка и внедрение международных стандартов и нормативных актов, регламентирующих использование ИИ в контексте защиты от интернет-мошенничеств, включая защиту данных пользователей и соблюдение этических норм.

– Этика и ответственность в применении ИИ – проведение исследований и разработка этических норм, регулирующих использование ИИ в сфере борьбы с интернет-мошенничествами, чтобы избежать возможных негативных последствий, таких как нарушение конфиденциальности, ошибки в определении угроз и избыточное вмешательство в частную жизнь.

МАЗМҰНЫ

Беттеу:
Туренова Б.

Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы ғылыми-зерттеу және редакциялық-баспа
жұмыстарын ұйымдастыру бөлімі
050060, Алматы қ., Өтепов көш., 29

Басуға 20 желтоқсан 2024 ж. жіберілді.
Пішімі 60х84 1/16 №1 баспаханалық қағаз.
Ризографтық басылыс. Есептік баспа табағы 4,9.
Таралымы 100.