Рисунок 6. Регистрация базы данных

Рисунок 7. Окно базы данных после подключения

1. Панова, Н. Ф. FireBird. Установка, разработка баз данных, реализация запросов: методические указания / Н. Ф. Панова. — Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014. — 45 с.
2. <https://besplatnye-programmy.com/raznoe-dlya-razrabotchikov/1095-ibexpert8239.html>

Поликарпова Д.Т., Редников Д.В.

Проблемы использования искусственного интеллекта в правоохранительных органах

ФГБОУ ВО «Баширский государственный университет»

(Россия, Уфа)

doi: 10.18411/trnio-12-2021-101

Аннотация

Правоохранительные органы являются неотъемлемой частью в системе защиты информации. В данной статье рассмотрено использование искусственного интеллекта в качестве борьбы с преступностью. Путем метода прогнозирования, вычисления вероятности, где и когда будет совершено преступление. А так же прописаны проблемы внедрения искусственного интеллекта и необходимость закрепления в правовое регулирование государства с целью национальной безопасности, а так же защиты данных.

Ключевые слова: правоохранительные органы, искусственный интеллект, проблемы, правовое регулирование.

Abstract

Law enforcement agencies are an integral part of the information security system. This article discusses the use of artificial intelligence in the fight against crime. By a prediction method, calculating the probability of where and when a crime will be committed. And also spelled out the problems of introducing artificial intelligence and the need to consolidate in the legal regulation of the state for the purpose of national security, as well as data protection.

Keywords: law enforcement, artificial intelligence, problems, legal regulation.

В современном обществе ежегодно обновляются, усовершенствуются информационные технологии. Масштабное использование современных методов обработки и хранения информации в вычислительной технике создало не только объективные предпосылки повышения уровня эффективности всех видов деятельности общества, но и ряд проблем в области информационной безопасности, связанные с появлением новых угроз нападения с целью хищения данных [3]. Информация на сегодняшний день имеет цену, каждая организация (здесь можно также говорить об государстве) в какой-либо сфере всеми усилиями старается обеспечить себе полноценную защиту.

Особую роль в обеспечении информационной безопасности личности, общества и государства по борьбе с компьютерными преступлениями и противодействию разведки играют правоохранительные и федеральные исполнительные органы такие как: МВД (Управление К), ФСБ, ФСТЭК, Прокуратура, ФТС. Основными функциями которых являются [2]:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации ;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации.

На сегодняшний день по указу Президента РФ были реализованы инвестиции и интерес к разработке технологий машинного обучения, которые лежат в основе возможностей искусственного интеллекта в промышленных, гражданских и военных сферах. Данные вложения в исследования и разработки в области ИИ способствовали росту инноваций и производительности, а также обострению конкуренции между западными странами в гонке за технологическое преимущество. Масштаб сбора и агрегации данных создают более широкие понятия связанные с рисками для обнаружения нарушения конфиденциальности и целостности. Помимо этого, существуют недостатки таких систем, из-за несовершенствования правового регулирования в правоохранительной сфере.

Для понимания проблемы, стоит обозначить алгоритм работы новой, интеллектуальной системы. Искусственный интеллект создается на основе открытых баз данных в обучении специализированных моделей, тем самым возникают риски воспроизведения и усиления систематических ошибок из неполных или неточных источников данных. Эта предвзятость может быть связана с явными и / или неявными предубеждениями, которые могут возникнуть из-за потенциально избирательного характера сообщений о преступлениях и расследований.

Применение искусственного интеллекта может быть использовано в качестве стратегии борьбы с преступностью, связанная комбинацией аналитических методов для получения оценки статистической вероятности того, где и когда будет совершено преступление. Прогнозирование можно классифицировать следующим способом:

- методы прогнозирования места и времени совершения преступлений;
- методы прогнозирования преступников и выявления лиц, которые могут совершить преступления;
- методы определения личности преступников;
- методы прогнозирования жертв преступлений.

Тем самым, можно предположить, что данный подход к раскрытию преступлений имеет высокий приоритет в развитии информационных технологий. И стоит обратить внимание на начальный этап разработки. Именно разработчик может халатно отнестись к заказу государственных нужд и внести систематические ошибки. Например, в современной истории существует факт о том, что система, работающая на ИИ произвела утечку персональных данных в открытую сеть Интернет. Данный инцидент произошел в следствии некомпетентной разработки нормативно-правовой базы.

Проблема также заключается в широком спектре использования данной технологии. В ниже приведенной таблице 1 прописывается применение искусственного интеллекта в совершении преступлений и иных противоправных действий [4].

Таблица 1

<i>Способ совершения преступления</i>	<i>Сфера применения</i>
<i>Фишинг</i>	<i>Посвяательства на собственность, неприкосновенность частной жизни, тайну переписки, хакерские атаки</i>
<i>Использование дронов</i>	<i>Посвяательства на жизнь, теракты, слежка, несанкционированная съемка, изучение объектов недвижимости с целью последующего проникновения, контрабанда наркотиков и других предметов, запрещенных или ограниченных в обороте, перемещение наркотиков, оружия, денег и пр. в места лишения свободы</i>
<i>Синтезирование фейковой информации</i>	<i>Дискредитация лиц, принимающих решения, шантаж, провоцирование паники</i>
<i>Использование автоматизированных автономных систем, управляемых искусственным интеллектом</i>	<i>Посвяательства на жизнь и здоровье, слежка</i>
<i>Использование ботов</i>	<i>Мошенничество, распространение наркотиков, порнографии, побуждение к самоубийству, посвяательства на половую неприкосновенность</i>

Указ Президента Российской Федерации от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" направлен на закрепление искусственного интеллекта в правовом секторе. Большого внимания заслуживает пункт, в котором расписывается о развитии Национальной стратегии, где определяются цели, задачи и обеспечение безопасности, для сохранения стратегических приоритетов государства.

Таким образом, для решения проблемы развития юридической силы ИИ должны соблюдаться следующие правила [1]:

- обеспечение защиты прав и свобод человека, гарантированный установленными российскими и международными законодательными актами прав и свобод человека;
- безопасность: предупреждение и уменьшение рисков возникновения негативных последствий применения технологий искусственного интеллекта, с целью недопустимости использования искусственного интеллекта для умышленного причинения вреда как гражданам, так и юридическим лицам;

- прозрачность: доступное описание работы искусственного интеллекта для ознакомления широких масс потребителей и разработчиков;
- технологический суверенитет: обеспечения материальной поддержки для создания отечественных технологий для разработки новых алгоритмов работы, основанные на ИИ;
- целостность инновационного цикла: обеспечение совместного взаимодействия научных исследований и аналитических секторов в области криминогенной обстановки страны;
- адаптация для отечественных государственных информационных систем.

Таким образом развитие и применение искусственного интеллекта в правоохранительной сфере произведет положительный эффект в борьбе с преступностью и противоправной деятельности. Для реализации полноценной его работы нужно учитывать все недостатки и разработать методику регулирования создания данной системы.

1. Указ Президента Российской Федерации от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации"
2. Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е. Основы информационной безопасности. Учебное пособие. – Иркутск, ФГОУ ВПО ВСИ МВД России, 2015, С. 21
3. Ларина Е. С. Искусственный интеллект. Большие данные. Преступность / Е. С. Ларина, В. С. Овчинский. — М. : Кн. мир, 2018. — С.162-164
4. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 753–766

Редников Д.В., Комарова М.А.

Проблемы формирования культуры кибербезопасности

*ФГБОУ ВО «Баширский государственный университет»
(Россия, Уфа)*

doi: 10.18411/trnio-12-2021-102

Аннотация

В статье проанализированы основные проблемы кибербезопасности в современных российских реалиях, рассмотрена необходимость формирования информационной культуры граждан для предотвращения нарушения их материальных и нематериальных прав.

Ключевые слова: кибербезопасность, информационная безопасность, информационные технологии.

Abstract

The article analyzes the main problems of cybersecurity in modern Russian realities, considers the need to form an information culture of citizens to prevent violations of their material and non-material rights.

Keywords: cybersecurity, information security, information technology.

Информатизация населения, организаций и государственной сферы является неизбежным этапом общественного прогресса, который сейчас активно проходит в российском обществе. Однако по мере распространения информационных технологий увеличивается и количество правонарушений в этом поле, в связи с чем в Российской Федерации в 2016 году принимается Доктрина информационной безопасности Указом Президента РФ от 5.12.2016 №646 [8], где ей указаны основные представления государства в области кибербезопасности, в частности, само понятие «информационная безопасность»