СЕКЦИЯ 5. ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ВОЙН

УДК 004

Бильданов С.З., Попов А.А.
Поволжский государственный университет телекоммуникаций и информатики, Самара

Научный руководитель:
Новикова Д.Д.
Поволжский государственный университет телекоммуникаций и информатики, Самара

СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В настоящей работе представлен анализ актуальности вызовов в области информационной безопасности, возникающих в направлениях обеспечения информационной безопасности в условиях информационных войн, обеспечения ИБ в сфере, обеспечение безопасности органов исполнительной власти, а также актуальность применения ИИ в сфере обеспечения ИБ.

Ключевые слова: информационная безопасность, искусственный интеллект.

Согласно Стратегии национальной безопасности РФ обеспечение информационной безопасности является одним из ключевых направлений обеспечения национальной безопасности [1]. Таким образом, тема нашей работы актуальна.

Целью нашей работы мы видим освещение основных вызовов информационной безопасности в различных областях. Мы решили рассмотреть следующие направления: обеспечение информационной безопасности в период информационных войн, обеспечение ИБ в сфере экономики, а также информационная безопасность органов исполнительной власти и применение ИИ в рамках обеспечения ИБ.

Постепенное развитие цифровых технологий несет за собой колоссальные риски и угрозы. В связи с этим в условиях геополитических изменений и цифровизации всех сфер жизнедеятельности человека, в правовой сфере необходимо проведение полномасштабных исследований и проработки современных подходов к систематизации информационного права.

На 2022 г. в информационном законодательстве существовал ряд проблем при обеспечении безопасности, такие как факт существования кибератак, как таковых, общественно-опасные деяния с использованием информационных средств, использование искусственного интеллекта и

робототехники в преступных целях. [1] В наше же время, на 2025 г.д вступил ряд изменений, направленных на усиление ответственности в области информационной безопасности, такие как повышение мер наказания по ст. 272–274 УК РФ [2], также повысилась мера ответственности за распространение ложной информации по ст. 207.3 УК РФ [3]. На основании приведенных сведений можно сделать вывод, что актуальность вызовов обеспечения информационной безопасности в условиях информационной войны снизилась, но не исчезла.

Прежде чем обеспечивать информационную безопасность, необходимо определить список угроз защищаемого субъекта. Информационная безопасность органов исполнительной власти включает в себя обеспечение их информационных потребностей в рамках их ответственности и в объемах, необходимых для выполнения возложенных задач, полноту, своевременность и достоверность информации, необходимой для принятия решений; безопасность информации и информационных ресурсов; безопасность информационного обмена [4].

В наше время возможно обеспечить безопасность информационного обмена, за счет построения защищенных информационных телекоммуникационных систем, с применением технических средств, сертифицированных ФСТЭК. Также стандартной процедурой является постановление соответствующего правового режима применяя различные политики безопасности, положения и прочее.

Однако, даже несмотря на серьезное покрытие законодательством проблем информационной безопасности субъектов и объектов КИИ, тем не менее некоторые проблемы до сих пор не урегулированы, например защита информации с грифом «Для служебного пользования». Несмотря на федеральные законы и указы Президента, регулирующие защиту информации для служебного пользования, ответственность за ее разглашения законодательно не регулируется. Следовательно, данный вопрос по-прежнему остается актуальным.

Стремительная информатизация и интеллектуализация общества породили вопрос применения систем на основе искусственного интеллекта, причем данное направление очень популярно с экономической точки зрения, так, с 2019 по 2025 г. мировой рынок технологий обеспечения информационной безопасности, использующей искусственного интеллекта, непрерывно рос и достиг оценочного показателя более 30 млн долларов [5].

Основными факторами, обуславливающими необходимость применения искусственного интеллекта, являются необходимость оперативного реагирования и нехватка квалифицированного персонала, а также факт использование злоумышленниками искусственного интеллекта при проведении атак на системы.

В рамках атаки зачастую применяют отвлекающие маневры, такие как сетевое сканирование или атаки типа «Отказ в обслуживании». Такие

атаки позволяют отвлечь сотрудников на их решение, «растягивая» фронт обороны и позволяя незаметно реализовать более серьезную атаку. В таких условиях, все более актуальна идея применения искусственного интеллекта, который способен обрабатывать значительные объемы информации и реагировать на инциденты даже в нерабочее время.

Для гарантии обеспечения требуемого уровня защиты информации внедряемой системой, необходимо ее корректно реализовать, внедрить и настроить. Причем в процессе настройки модели подвержены угрозам отравления данных и атаки уклонения.

Обе эти угрозы связаны с искажением данных для обучения модели, при отравлении данных переданная выборка искажена до момента обучения системы, во второй угрозе искажение данных происходит в процессе обучения путем незаметных видоизменений корректных входящих данных. В процессе таких атак система обучается некорректно и может работать в пользу третьих лиц, значительно понижая уровень защищенности информации.

Классические интеллектуальные системы, используемые в области информационной безопасности сконструированы на основе анализа отклонений объема специфического трафика, неуспешных попыток аутентификации, шаблонов работы пользователей, идентификации скомпрометированных учетных записей.

Список использованных источников:

1. Дубень А.К. Аспекты и угрозы информационной безопасности в эпоху современных информационных войн // Вестник Удмуртского университета. Серия «Экономика и право». 2022. № 6. URL: https://cyberleninka.ru/article/n/aspekty-i-ugrozy-informatsionnoy-bezopasnosti-v-epohu-sovremennyh-informatsionnyh-voyn (дата обращения: 29.04.2025).

2. КонсультантПлюс: УК РФ Глава 28. Преступления в сфере компьютерной информации: сайт / Региональный центр правовой информации Информправо. М., 1997–2020. URL: http://www.consultant.ru/ (дата обращения: 29.04.2025).

3. КонсультантПлюс: УК РФ Статья 207.3. Публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации или войска национальной гвардии Российской Федерации: сайт / Региональный центр правовой информации Информправо. М., 1997–2020. URL: http://www.consultant.ru/ (дата обращения: 29.04.2025).

4. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал

российского права. 2015. № 8 (224). URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-organov-ispolnitelnoy-vlasti-na-sovremennom-etape (дата обращения: 29.04.2025).

5. Шананин В.А. Применение систем искусственного интеллекта в защите информации // Инновации и инвестиции. 2022. № 11. URL: https://cyberleninka.ru/article/n/primenenie-sistem-iskusstvennogo-intellekta-v-zaschite-informatsii (дата обращения: 29.04.2025).

Bildanov S.Z., Popov A.A.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Novikova D.D.
Volga Region State University of
Telecommunications and Informatics, Samara

CONTEMPORARY CHALLENGES IN THE FIELD OF INFORMATION SECURITY

Abstract. This paper presents an analysis of the relevance of challenges in the field of information security arising in the areas of ensuring information security in the context of information wars, ensuring information security of executive authorities, as well as the relevance of the use of AI in the field of ensuring information security.

Keywords: information security, artificial intelligence.