УДК 37.378.046.4

Овчаренко Марина Сергеевна, к.т.н., доцент,
Военный институт (инженерно-технический)
ВА МТО им. генерала армии А.В. Хрулёва,
г. Санкт-Петербург

АНАЛИЗ СОВРЕМЕННЫХ И ВОЗМОЖНЫХ УГРОЗ БЕЗОПАСНОСТИ РОССИИ
THE ANALYSIS OF CURRENT AND POSSIBLE THREATS TO RUSSIA'S SECURITY

Аннотация: обзорная статья в которой представлен анализ современных и возможных угроз нашей стране; из предоставленных результатов видно, что анализ угроз национальной безопасности страны является предметом серьезного изучения; некоторые из ключевых угроз, выявленных в исследованиях, включают в себя появления оружия на новых физических принципах, киберугрозы, терроризм, экономические угрозы, а также угрозы в области информационной безопасности и применения искусственного интеллекта.

Abstract: the article presents an analysis of current and possible threats to our country; from the results provided, it can be seen that the analysis of threats to the national security of the country is the subject of serious study; some of the key threats identified in the research include the emergence of weapons based on new physical principles, cyber threats, terrorism, economic threats, as well as threats in the field of information security and the use of artificial intelligence.

Ключевые слова: конвенциональное вооружение, системы искусственного интеллекта (ИИ), нейросети, киберугрозы, риски, кибератаки.

Keywords: conventional weapons, artificial intelligence (AI) systems, neural networks, cyber threats, risks, cyber attacks.

Ускорение процесса совершенствования вооружений стало особенно заметным в последние два столетия, когда боевые свойства оружия, его поражающее действие стали определяться достигнутым уровнем науки, результатами научных исследований, появлением новых технологий и материалов. Это, в свою очередь, закономерно определяло соответствующие изменения форм и способов вооруженной борьбы, которые зарождались и развивались в ходе ведения боевых действий.

Отметим, что в XX столетии на мировую арену вышли принципиально новые виды оружия – химическое, биологическое, ядерное, способные наносить массовое поражение.

Очередной качественный скачок в изменении содержания и развитии форм и способов вооруженной борьбы отмечается в XXI веке, связанный с тенденциями появления оружия на новых физических принципах, особенно на стратегическом и оперативном уровне. В настоящее время к современным средствам поражения относится конвенциональное вооружение (КВ).

КВ – обычное вооружение, которое не относится к оружию массового поражения, такому как ядерное, химическое или биологическое оружие. Следовательно, вооруженный конфликт между двумя или несколькими государствами, ведущийся в соответствии с нормами международного права – это на текущий момент конвенциональная война [1, 2]. В такой войне противники придерживаются общих правил ведения войны, а также отказываются от использования запрещенных мер [1].

Конвенциональное вооружение может включать в себя различные виды оружия, такие как авиационное, наземное, морское, а также высокоточное оружие [1]. Считается, что стратегическое конвенциональное оружие (СКО) – это оружие, которое может нанести значительный ущерб противнику, но не относится к оружию массового поражения [2].

Существует множество видов конвенционального оружия, которые могут быть использованы в военных конфликтах (рисунок 1):

Рис. 1. Общие виды конвенционального вооружения (КВ)

Конвенциональное вооружение играет важную роль в современных военных конфликтах и может быть использовано в различных ситуациях, от локальных конфликтов до глобальных войн [1]. Однако, очень важно соблюдение международного права и правила ведения войны, чтобы минимизировать гражданские жертвы и разрушения. Конечный список видов конвенционального оружия может быть гораздо больше (рисунок 2), но перечисленные выше являются наиболее распространенными.

Рис. 2. Расширенный список видов КВ и динамика его развития

Следующим видом современных средств поражения можно считать различные методы кибернетического нападения (кибератаки) [4].

Существует множество методов кибернетического нападения, которые могут быть использованы для получения несанкционированного доступа к информации, уничтожения данных или манипуляции с ними. Рассмотрим более подробно каждую из них:

Взломы – это метод, при котором злоумышленник получает несанкционированный доступ к защищенной информации или системе. Взломы могут осуществляться с помощью уязвимостей в программном обеспечении, социальной инженерии или использования слабых паролей.

Вирусы – это программы, которые могут распространяться через сеть и заражать компьютеры, могут использоваться для уничтожения данных, манипуляции с ними или получения несанкционированного доступа к системе.

Фишинг – это метод, при котором злоумышленник пытается получить доступ к конфиденциальной информации, такой как пароли или номера кредитных карт, путем манипуляции пользователем. Фишинг может осуществляться через электронную почту, социальные сети или веб-сайты.

Денайал-оф-сервис (DDoS) – это метод, при котором злоумышленник перегружает сеть или сервер, что приводит к отказу в обслуживании. DDoS может использоваться для вымогательства или манипуляции с информацией.

Мальварь – это общее название для вредоносных программ, которые могут использоваться для уничтожения данных, манипуляции с ними или получения несанкционированного доступа к системе. Мальварь может распространяться через электронную почту, веб-сайты или съемные носители.

Нападение на хвост – это метод, при котором злоумышленник использует поддельный бейдж с маркировкой, схожей с теми, что выдает целевая организация, чтобы получить доступ к охраняемой зоне.

Кибершпионаж – это метод, при котором злоумышленник получает доступ к конфиденциальной информации, такой как планы, документы или секреты, путем взлома системы или использования социальной инженерии.

Социальная инженерия – это метод, при котором злоумышленник пытается манипулировать человеческими слабостями, чтобы получить доступ к конфиденциальной информации. Социальная инженерия может осуществляться через электронную почту, телефон или личное общение.

В целом, кибератаки могут воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака, обычно, поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя. Примеры существующих интерактивных карт кибератак представлены на рисунке 3.

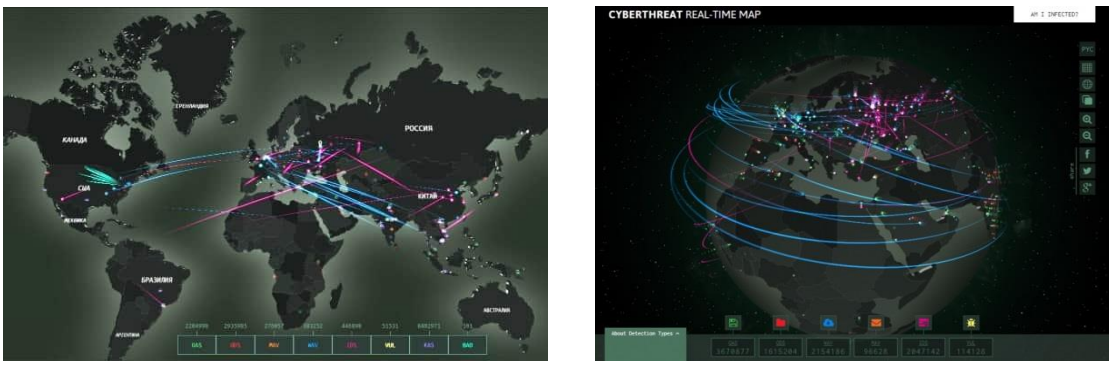


Рис. 3. Интерактивная карта кибератак в реальном времени

Для защиты от кибернетических нападений необходимо использовать различные меры, включая использование антивирусного программного обеспечения, установку обновлений безопасности, использование сложных паролей, обучение персонала, работающего с информацией, и использование многофакторной аутентификации.

Кроме того, на государственном уровне должны приниматься меры для защиты от возможных угроз, связанных с кибернетическими нападениями, и разрабатываться стратегии для использования кибернетических технологий в безопасных целях [4].

Сегодня к современным средствам поражения можно отнести биологическое оружие и изучение возможных угроз, связанных с биологическими агентами и пандемиями. Оружие биологическое (бактериологическое) – вид оружия массового поражения, действие которого основано на использовании болезнетворных свойств микроорганизмов и продуктов их жизнедеятельности (далее биологическое оружие) [5].

Несмотря на то, что создание биологического оружия доступно многим государствам, массового применения его до сих пор не наблюдалось. С 1975 года вступила в силу Конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении от 1972 года [6].

Но изучение возможных угроз, связанных с биологическими агентами и пандемиями, является важной задачей для обеспечения национальной безопасности нашей страны. В настоящее время специалисты в России и других странах обсуждают возможные биологические угрозы, в том числе искусственно созданные, и предлагают новые подходы к регулированию биобезопасности и биозащищенности своих стран [6].

Уже известно, что некоторые проекты Пентагона в США направлены на изучение возможных агентов биологического оружия, в том числе возбудителей пандемий [5]. В связи с этим, важно развивать научные и технологические возможности для обнаружения и борьбы с биологическими угрозами [6].

Возможными способами применения биологического оружия на сегодняшнее время являются [6]:

– заражение аэрозольными биологическими средствами приземного слоя воздуха;

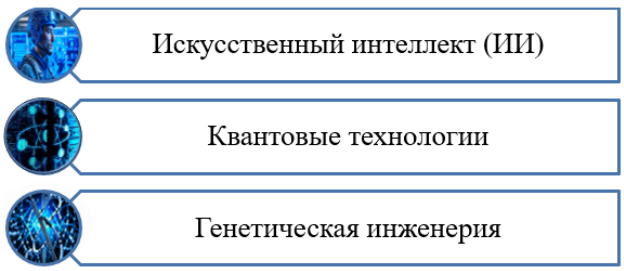
– рассеивание в отдельных районах, искусственно заражённых биологическими средствами кровососущих насекомых – переносчиков инфекционных болезней;

– заражение биологическими средствами воздуха, воды и продовольствия и т.д.

Высокая эффективность биологического оружия обусловлена малой инфицирующей дозой, скрытностью применения на больших территориях, трудностью индикации, избирательностью действия, сильным психологическим воздействием, сложностью биологической защиты войск и населения и ликвидации последствий применения.

В целом, изучение возможных угроз, связанных с биологическими агентами и пандемиями, является важной задачей для обеспечения национальной и мировой безопасности. Необходимо продолжать научные исследования и развивать технологии для обнаружения и борьбы с биологическими угрозами, а также принимать меры для обеспечения биологической безопасности.

На современном этапе перспективными угрозами являются:



По прогнозам исследователей, искусственный интеллект станет важнейшей частью современной войны. И одной из главных причин в пользу этого является тот факт, что ИИ способен крайне эффективно обрабатывать большие объёмы входящих данных.

В продолжение исследования рассмотрим потенциал квантовых вычислений и криптографии, а также возможных угроз, связанных с этими технологиями.

Квантовые технологии – это область физики и инженерии, которая использует специфические особенности квантовой механики, такие как квантовая запутанность, квантовая суперпозиция и квантовое туннелирование, для создания новых технологий и устройств. Они могут использоваться в различных областях, включая криптографию, молекулярную моделирование, оптику, электронику, медицину и т.д.

В целом, квантовые технологии представляют собой перспективную область, которая может привести к созданию новых технологий и устройств, но также может представлять угрозу для безопасности. Уже на этом этапе необходимо принимать меры для защиты от возможных угроз, связанных с использованием квантовых технологий, и разрабатывать стратегии для использования их в безопасных целях.

Сегодня широко известно понятие генетической инженерии, как совокупности методов и технологий, используемых для изменения генетического материала организмов. Она включает в себя получение рекомбинантной ДНК и РНК, выделение генов из организмов, манипуляции с генами, введение их в другие организмы и выращивание искусственных организмов после удаления выбранных генов из ДНК [7].

Генная инженерия уже используется в различных областях, включая медицину, сельское хозяйство, промышленность и науку. Например, генная инженерия уже используется в создании новых лекарств, получения растений и животных, устойчивых к вирусам, и создания новых видов бактерий.

Однако, генная инженерия может вызывать этические и социальные проблемы, такие как создание генетически модифицированных организмов, которые могут иметь непредсказуемые последствия для окружающей среды и здоровья людей (новые и опасные вирусы, непредвиденные новые опасные вещества, несовершенные технологии).

Поэтому, также должны уже сейчас приниматься меры для регулирования использования генной инженерии и защиты от возможных угроз, связанных с ее использованием.

В целом, изучение возможных угроз на современном этапе, является важной задачей для обеспечения национальной и мировой безопасности. Необходимо продолжать научные исследования в данном направлении с целью поиска путей для предупреждения и борьбы с ними.

Список литературы:

1. Аничкина Т. Конвенциональное высокоточное оружие в современном стратегическом контексте. Мировая экономика и международные отношения, 2012, № 5, сс. 103-111. https://doi.org/10.20542/0131-2227-2012-5-103-111
2. Цымбал В.И. Высокоточное оружие в системе современных средств вооруженной борьбы. НИА Наследие отечества (http://old.nasledie.ru/persstr/persona/cimbal/article.php?art=3).
3. Военный энциклопедический словарь. Под ред. Н. Огаркова. М., 1984. С. 159.
4. Кибератаки: статья [Электронный ресурс]: https://www.tadviser.ru/index.php/ (дата обращения: 02.12.2023 г.).
5. Термины МЧС России: Оружие биологическое (бактериологическое) [Электронный ресурс]: https://mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/2274 (дата обращения: 02.12.2023 г.).

6. Официальные Сайт Организации объеденных наций Конвенция о биологическом оружии. Конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении [Электронный ресурс]: https://disarmament.unoda.org/ru/wmd/биологическое-оружие/ (дата обращения: 02.12.2023 г.).

7. Ремизова Р. Что такое генная инженерия и зачем вмешиваться в природу организмов: подробнее на РБК: [Электронный ресурс]: https://trends.rbc.ru/trends/futurology/612f77ad9a7947ce386b68ba (дата обращения: 02.12.2023 г.).

8. Овчаренко М.С. К развитию профессиональных навыков у курсантов военных вузов в сфере технологий искусственного интеллекта //Сборник статей Международной научной конференции "Безопасность: Информация, Техника, Управление" (Санкт-Петербург, апрель 2022 г.) – СПб.: ГНИИ "Нацразвитие", 2022. – С. 42-44.