**Юсуфзода И.М**

**Магистрант 2 курс**

**Научный руководитель: Макаров И.С.,к.п.и. ,доцент**

**Поволжский государственный университет телекоммуникаций и информатики**

# ИНТЕГРАЦИЯ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ В СФЕРУ КИБЕРБЕЗОПАСНОСТИ: СЕТЕВЫЕ СИМУЛЯЦИИ И АНАЛИЗ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

**Аннотация:** Вычислительные модели когнитивных процессов могут использоваться в инструментах кибербезопасности, экспериментах и симуляциях для решения проблем человеческого участия и эффективного принятия решений по обеспечению безопасности вычислительных сетей. В данной статье будет рассмотрен механизм моделирования сетевых атак.

**Ключевые слова**: кибербезопасность, сетевые симуляции, киберсимуляция, компьютерное моделирование, пользователь.

Yusufzoda.I.M

# Integrating Cognitive Modeling into Cybersecurity: Network Simulations and User Behavior Analysis

**Abstract:** Computational models of cognitive processes can used in cybersecurity tools, experiments and simulations to solve problems of human participation and effective making decisions to ensure the security of computer networks. IN This article will discuss the mechanism for modeling network attacks.

**Keywords:** cybersecurity, network simulations, cyber simulation, computer modeling, user.

Когнитивное моделирование может решать междисциплинарные задачи кибербезопасности, требующие сквозных подходов в области

гуманитарных и вычислительных наук, таких как следующие: а) состязательное мышление и теория поведенческих игр для прогнозирования субъективной полезности атакующего и распределения вероятности принятия решения, б) человеческий фактор киберинструментов для решения проблем интеграции человека в систему, оценки когнитивных состояний защитника и возможностей автоматизации, в) динамическое моделирование с участием моделей атакующего, защитника и пользователя для улучшения исследований киберпэдемиологии и кибергигиены, и г) исследования эффективности обучения и сценарии обучения для решения проблем кибербезопасности среди людей, развития навыков в области кибербезопасности и эффективного принятия решений. Модели могут быть первоначально построены на уровне группы на основе средних тенденций подгруппы каждого субъекта, на основе известных статистических данных, таких как уровень владения конкретными навыками, демографические характеристики и культурные факторы. Для более точных прогнозов когнитивные модели могут быть точно настроены для каждого отдельного атакующего, защитника или профиля пользователя и обновляться с течением времени (на основе зарегистрированного поведения) с помощью таких методов, как трассировка модели и динамическая подгонка параметров.

Компьютерное моделирование имеет большое значение в области кибербезопасности. Симуляции полезны в качестве компонентов программного обеспечения сетевой безопасности и в учебных упражнениях для специалистов по безопасности, а также в качестве вспомогательных программных средств, предназначенных для пользователей сети. Более того, многие фундаментальные исследования в области человеческого фактора, связанного с киберпространством, и киберэпидемиологии выигрывают от программного обеспечения для моделирования. Динамика кибербезопасности в основе своей человеческая и состязательная, охватывающая целый ряд взаимодействий атакующего, защищающегося и

пользователя. Моделирование человеческого познания и поведения имеет особое значение для учета характеристик этой предметной области. [2, с. 1065]

Сетевые симуляции, включающие высокоточные модели пользователей, атакующих и / или защитников, могут использоваться для запуска обучающих сценариев с реалистичным трафиком и уязвимостями, созданными пользователями. Сбор и анализ данных, полученных в результате выполнения этих симуляций, предоставляет средства для изучения того, как различные изменения в инструментах, ограничениях безопасности и обучении могут повлиять на общую сетевую безопасность. Модели познания пользователей и защитников могут использоваться для оценки их когнитивных состояний в режиме реального времени, чтобы решать проблемы интеграции человеческих систем и определять задачи, которые выиграли бы от автоматизации. Модели познания злоумышленников могут использоваться в дополнение к теории поведенческих игр для прогнозирования полезности субъективных действий и оптимальных путей защитных действий. Точно так же, как симуляции в здравоохранении предсказывают, как может распространяться эпидемия и способы ее сдерживания, такие симуляции могут использоваться в области кибербезопасности как средство прогресса в изучении сетевых атак.

Многие предположения, сделанные системными администраторами и кодифицированные в качестве политик безопасности и передовых практик, основаны на неподтвержденных данных и часто разрабатываются в ответ на тематические исследования предыдущих инцидентов в рамках управления реагированием на инциденты. Такие рекомендации сложно протестировать эмпирически, и они, вероятно, будут варьироваться в зависимости от типа и размера сети. Ослабление ограничений, чтобы увидеть, насколько уязвимой становится сеть в реальных условиях, является безответственным. Повсеместное ужесточение ограничений также не всегда приводит к

желаемым результатам, поскольку введение дополнительных политик и ограничений может запретить законную работу и увеличить вероятность непреднамеренного воздействия пользователей на сеть. Однако моделирование сети и ее пользователей дает возможность тестировать различные сетевые политики без реальных последствий. Такое моделирование может использоваться для выявления пробелов в процедурах и потенциально нелогичных рекомендаций. [1, с. 99]

Например, предположения о занесении в черный или белый списки определенных веб-сайтов, номеров портов и программного обеспечения могут быть рассмотрены в контексте реалистичных моделей поведения пользователей и сетевой активности. Даже самые традиционные суждения системного администратора могут основываться на непроверенных предположениях, таких как идея о том, что определенные требования к сложности пароля повышают общую безопасность системы. Однако некоторые когнитивные ограничения (например, производственная предвзятость, ограничение памяти) могут заставить пользователей мошенничать, храня пароли в незашифрованных текстовых файлах или используя визуальные шаблоны клавиатуры или другие общие шаблоны. Высокоточные пользовательские модели могут помочь в прогнозировании такого поведения, а высокоточное сетевое моделирование может предсказать, как взаимодействие ограничений и поведения может повлиять на общую гигиену сети. Более того, тестирование множества потенциальных параметров может помочь в поиске почти оптимальной конфигурации для ограничений и других политик.

Текущие процедуры обучения могут по-разному влиять на разные типы пользователей. Высококачественная киберсимуляция должна учитывать индивидуальные различия пользователей. С помощью такого моделирования можно обнаружить, что определенные процедуры обучения в целом улучшают работу сетей по сравнению с другими. [3, с. 125]

Наконец, процессные модели познания и поведения могут помочь лучше понять умы кибератакующих, защитников и пользователей, что еще больше улучшит сетевую безопасность. Недавние исследования показывают, что моделирование и прогнозирование психического состояния и решений злоумышленников может привести к улучшению вспомогательных средств для принятия решений и более высокому уровню предотвращенных атак. Интеллектуальное состояние защитника в значительной степени игнорируется в инструментах кибербезопасности, хотя исследования в области кибернетики и автоматизации показывают, что когнитивное моделирование может оказать большую помощь и в этой области. Современные лучшие примеры прогнозирования поведения сетевых пользователей основаны на статистическом анализе для прогнозирования обычных и необычных сроков и мест доступа. Модели вычислительных процессов познания пользователей могут помочь преодолеть классификацию обычного / необычного поведения пользователей и предсказать потенциальные ошибки, которые приводят к угрозам безопасности. Исследования показывают, что эффективность обучения защитников / пользователей также может быть повышена с помощью инструментов, основанных на когнитивном моделировании.

Список литературы

1. Классификация DDoS-атак на основе нейросетевой модели / Р. М. Мухаматханов, А. А. Михайлов, Б. И. Баянов, М. В. Тумбинская // Прикладная информатика. - 2019. - Т. 14, № 1(79). - С. 96-103.

2. Новикова, Е. С., Федорченко, Е. В., Котенко, И. В., & Холод, И. И. (2023). Аналитический обзор подходов к обнаружению вторжений, основанных на федеративном обучении: преимущества использования и открытые задачи. Информатика и автоматизация, 22(5), 1034-1082.

3. Овчинникова Елена Сергеевна (2021). Графовые модели динамики реализации сетевых атак в автоматизированных системах органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки, 48 (1), 119-129.