Аннотация – документ служит анализом ключевой роли женщин в области кибербезопасности, выявляя их вклад в различные отрасли и тонко указывая на то, как они несли нагрузку все это время. Анализ затрагивает несколько ключевых аспектов, включая исторический контекст и технологии, и методологии, разработанные женщинами в сфере кибербезопасности или оказавшие на них значительное влияние, с акцентом на их технологические достижения, которые не позволили отрасли погрузиться в тёмные века. Дополнительно исследуется влияние женщин на кибербезопасность в различных секторах, таких как "умные города", железные дороги, морское судоходство, фармацевтика / биотехнологии и кибербезопасность, демонстрируя их неоспоримое влияние на эти отрасли.

Документ обеспечивает синтез различных аспектов, предлагая ценную информацию для специалистов в области безопасности и специалистов из различных отраслей. Понимая уникальный вклад и перспективы женщин в кибербезопасность, заинтересованные стороны могут, наконец, начать осознавать важность разнообразия в усилении мер безопасности и стимулировании инноваций. Анализ необходим для разработки более инклюзивных стратегий безопасности, совершенствования отраслевой практики и вдохновения следующего поколения профессионалов в области кибербезопасности.

I. Введение

В постоянно развивающемся мире кибербезопасности женщины наконец-то проявили инициативу, чтобы показать всем, как это делается. Исторически недопредставленные, женщины сейчас оставляют заметный след, и, по прогнозам, к 2025 году они составят 30 процентов глобальной рабочей силы по кибербезопасности, а к 2031 году – 35 процентов, что представляет собой рост сектора безопасности.

Женщины в сфере кибербезопасности представляют собой сокровищницу опыта и инноваций, решая сложную задачу обеспечения безопасности цифрового ландшафта с изяществом, которого так не хватало. Их вклад охватывает различные области, от разработки безопасных технологий "умного города" до кибербезопасности критически важных секторов инфраструктуры, таких как железные дороги и морское судоходство. Они стремятся к созданию более инклюзивной и разнообразной рабочей среды, которая, как ни странно, имеет решающее значение для развития креативности и комплексного решения проблем.

A. Женщины-первопроходцы инноваций в области кибербезопасности

Мишель Дролет, как основатель и генеральный директор Towerwall, она изменила правила игры в формировании практик информационной безопасности и повышении осведомлённости благодаря своим экспертным взглядам. Керен Элазари, этичный хакер и исследователь, которая не только подчёркивает важность этичного взлома, но и вдохновляет следующее поколение профессионалов в области кибербезопасности своими увлекательными беседами и исследованиями. Мэй Ленг Там, главный сотрудник по инфобезопасности Министерства развития и окружающей среды Сингапура, которая руководит инициативами в области кибербезопасности в различных ведомствах и помогает им разрабатывать надёжные стратегии кибербезопасности и защиты данных.

Вклад женщин в кибербезопасность не ограничивается руководящими ролями. Они также находятся на передовой разработки новаторских технологий и методологий. Например, Авивит Котлер, CISO и DPO в Clalit Health Services, является экспертом в области управления рисками и обеспечения непрерывности бизнеса, обеспечивая безопасность конфиденциальных медицинских данных. А Сэм Кинг, генеральный директор Veracode, значительно улучшила безопасность приложений, сделав её важнейшим компонентом современных методов кибербезопасности.

Конечно, несмотря на весь этот прогресс, проблемы сохраняются. Гендерные предубеждения и стереотипы по-прежнему преобладают в этой области, часто отворачивая женщин от карьеры в сфере кибербезопасности. Однако инициативы инклюзивности, такие как программы наставничества и образовательные возможности, помогают преодолеть этот разрыв. Организации все больше осознают ценность различных команд для более эффективного выявления рисков кибербезопасности и их устранения.

B. Мотивация

Разнообразие и инклюзивность — это не просто модные слова; это секретный соус к эффективной безопасности. По мере того, как цифровой мир становится все более запутанным и сложным, потребность в свежих перспективах и инновационных решениях становится более актуальной, чем когда-либо. Привлекая внимание к вкладу женщин в кибербезопасность, этот анализ направлен на:

- **Продвижение разнообразие**: большее гендерное разнообразие в кадрах по кибербезопасности как разнородные команды необходимы для эффективного решения проблем и могут предвидеть и смягчать более широкий спектр киберугроз, чем обычные однородные группы.

- **Будущие поколения**: образец для подражания молодым женщинам и девушкам, рассматривающим карьеру в сфере безопасности. Подчёркивая отраслевые достижения женщин, существует возможность вдохновить следующее поколение на новые свершения.
- **Устранение гендерных предубеждений**: Разрушение барьеров является первым шагом к созданию более инклюзивной и благоприятной среды для всех специалистов по кибербезопасности.
- **Отраслевые практики**: предложение ценной информации, которая может помочь организациям разработать инклюзивные стратегии безопасности и улучшить отраслевые практики и наконец, отказаться от своих устаревших методов и принять более эффективный подход к кибербезопасности.

II. Женщины в сфере кибербезопасности

A. *Уровень недопредставленности*

1) *Морская промышленность*

- Женщины значительно недопредставлены в отрасли, в том числе на должностях, связанных с кибербезопасностью – только около 2% из 2 миллионов сотрудников в мире.
- Предпринимаются усилия по увеличению гендерного разнообразия, такие как ежегодный Международный день женщин-моряков IMO в целях повышения осведомлённости и Региональная стратегия Тихоокеанского сообщества в интересах женщин-моряков Тихоокеанского региона.
- Проблемы включают отсутствие политики, учитывающей гендерные аспекты, дискриминацию и отсутствие надлежащего оборудования для обеспечения безопасности женщин на судах.
- Такие организации, как Женская международная ассоциация судоходства и торговли (WISTA), работают над поддержкой и продвижением женщин на море, в том числе в сфере кибербезопасности.

2) *Умные города*

- Женщины играют решающую роль в разработке технологий "умного города", включая кибербезопасность. Анджана Раджан - специалист по правам человека, работающий над безопасными решениями для умных городов.
- Однако индустрия в целом сталкивается со значительным гендерным разрывом. Необходимы усилия по привлечению большего числа женщин в области STEM, которые способствуют развитию умных городов.
- Безопасность жизненно важна для умных городов, которые интегрируют множество взаимосвязанных систем, и важно иметь различные точки зрения от женщин-экспертов по безопасности.

3) *Железнодорожная отрасль*

- В железнодорожной отрасли традиционно доминировали мужчины, но женщины все чаще приходят в эту сферу, в том числе на должности по кибербезопасности.
- UNIFE, Европейская ассоциация железнодорожной отрасли, имеет Консультативную группу по вопросам гендерного равенства, продвигающую разнообразие и подчёркивающую возможности для женщин на железнодорожном транспорте.

4) *Фармацевтика/Биотехнологии*

- Более широкие области STEM, охватывающие эти отрасли, сталкиваются с аналогичными гендерными разрывами.
- Поощрение участия в STEM-образовании с раннего возраста имеет решающее значение для увеличения представленности женщин в сфере безопасности во всех биотехнологических отраслях.
- Привлечение женщин-экспертов по может дать ценные рекомендации по обеспечению безопасности конфиденциальных медицинских данных / научных исследований и защите критически важных систем в этих отраслях.

B. *Технологии и безопасность*

- **Искусственный интеллект:** Тереза Пейтон, бывший ИТ-директор Белого дома и генеральный директор Fortalice Solutions, подчеркнула рост угроз, связанных с искусственным интеллектом, включая мошенничество и дипфейки, связанные с использованием искусственного интеллекта для создания реалистичных поддельных идентификационных данных, что создаёт серьёзные проблемы для систем кибербезопасности. Пейтон подчёркивает необходимость надёжных протоколов безопасности и совместных стратегий защиты для противодействия этим возникающим угрозам.
- **Человекоцентричная кибербезопасность:** Доктор Джессика Баркер, соучредитель и со-генеральный директор Cygenta, уделяет особое внимание человеческой стороне безопасности. Она выступает за повышение осведомлённости о безопасности, улучшение поведения и культуры в организациях. Работа Баркер подчёркивает важность понимания человеческой психологии и социологии в области кибербезопасности, расширяя возможности людей эффективно распознавать киберугрозы и смягчать их последствия. её усилия включают проведение информационных сессий и конспектов для широкой аудитории, а также написание книг по безопасности.
- **Трансформация кибербезопасности:** Кирстен Дэвис, CISO Unilever, известна своим опытом в области совершенствования организационной культуры и трансформации кибербезопасности. Она руководила инициативами по совершенствованию процессов обеспечения безопасности и методов

работы во многих глобальных компаниях. Подход предполагает оптимизацию методов обеспечения безопасности в соответствии с бизнес-целями и укрепление культуры безопасности в организациях.

- **Резервное восстановление и ИИ-угрозы:** Сара Армстронг-Смит, главный советник по безопасности Microsoft в регионе EMEA, сыграла важную роль в решении проблем резервного восстановления, защиты и конфиденциальности данных. Она подчёркивает важность учёта достоверности информации при принятии решений, особенно в контексте угроз, порождаемых искусственным интеллектом, таких как deepfakes и смешанная реальность. Армстронг-Смит также подчёркивает необходимость того, чтобы организации опережали развивающиеся угрозы, используя искусственный интеллект и машинное обучение в своих стратегиях кибербезопасности.
- **Угрозы идентификации:** Тереза Пейтон также обсуждает меняющийся ландшафт угроз идентификации, включая возможность взлома умных зданий и их блокировки. Она подчёркивает важность понимания и смягчения этих угроз с помощью инновационных мер безопасности и стратегий влияния на безопасность.
- **Разнообразие и инклюзивность:** Линн Дом, исполнительный директор организации "Женщины в кибербезопасности" (WiCyS), является решительным сторонником разнообразия и инклюзивности в сфере кибербезопасности. Она подчёркивает важность политики DEI в преодолении кадрового разрыва и улучшении набора, удержания и продвижения женщин в сфере безопасности. Усилия направлены на создание эффективной индустрии безопасности.

C. Сферы, связанные с искусственным интеллектом

- **Мира Мурати:** как технический директор OpenAI сыграла важную роль в разработке и внедрении новаторских технологий искусственного интеллекта, таких как ChatGPT, DALL-E и Codex. Она подчёркивает важность общественного тестирования и ответственного использования искусственного интеллекта, выступая за его регулирование для обеспечения соответствия соответствовали человеческим намерениям. Её руководство помогло OpenAI стать лидером в области генеративного ИИ, расширяя границы того, чего может достичь ИИ, сохраняя при этом акцент на этических соображениях.
- **Линда Яккарино:** генеральный директор X (ранее Twitter), использует искусственный интеллект для расширения возможностей платформы, особенно в области проверки фактов и модерации контента. Она представила функцию краудсорсинга для проверки фактов, которая направлена на повышение точности и достоверности цифрового контента. Эта инициатива подчёркивает потенциал ИИ в борьбе с дезинформацией и повышении доверия к онлайн-платформам.
- **Сара Армстронг-Смит:** главный советник по безопасности Microsoft в регионе EMEA, фокусируется на пересечении искусственного интеллекта и кибербезопасности. Она рассматривает проблемы, связанные с угрозами, создаваемыми искусственным интеллектом, такими как глубокие подделки, и подчёркивает важность аварийного восстановления, защиты данных и конфиденциальности. Армстронг-Смит выступает за интеграцию искусственного интеллекта в стратегии кибербезопасности, чтобы опережать развивающиеся угрозы, обеспечивая использование технологий искусственного интеллекта для повышения безопасности и устойчивости.
- **Керен Элазари:** аналитик и исследователь в области безопасности, пропагандирует этичное использование искусственного интеллекта и хакерский менталитет для стимулирования инноваций в области кибербезопасности. Она подчёркивает важность этичного взлома и программ багхантинга и смягчения уязвимостей, связанных с искусственным интеллектом. Работа Элазари по созданию сообщества этичных хакеров и её пропаганда увеличения представительства женщин в сфере кибербезопасности имеют решающее значение для разработки надёжных мер безопасности искусственного интеллекта.
- **Кэтрин Лиан:** генеральный менеджер и технологический лидер IBM ASEAN, находится на передовой интеграции искусственного интеллекта в бизнес. Она подчёркивает необходимость повышения квалификации работников для эффективного использования искусственного интеллекта, гарантируя, что искусственный интеллект дополняет, а не заменяет человеческую работу. Усилия Lian по продвижению образования в области искусственного интеллекта и ответственного управления искусственным интеллектом необходимы для укрепления доверия к технологиям искусственного интеллекта и подготовки к будущим нормативным требованиям.

D. Влияние женщин в разных отраслях:

1) Морская отрасль:

Женщины добиваются значительных успехов в морской отрасли, особенно в усилении мер кибербезопасности. Например, такие инициативы, как Международная морская организация (IMO) и Женская международная ассоциация судоходства и торговли (WISTA), активно продвигают гендерное разнообразие и вовлечение в работу по обеспечению морской кибербезопасности. Эти организации подчёркивают важность кибербезопасности для защиты судовых и береговых систем от киберугроз, и женщины все чаще берут на себя руководящие роли в продвижении этих инициатив.

- **Трейси Эдвардс** – первая женщина, возглавившая женский экипаж в кругосветной гонке Whitbread (ныне Volvo Ocean Race) в 1989–1990 годах.
- **Неннетт Занде** – Разработала Aqua-Tractor, транспортное средство-амфибию, используемое для уборки пляжей и ликвидации разливов нефти.
- **Влияние**: Женщины возглавляют усилия по обеспечению безопасности морских операций, защищая корабельные и береговые системы от киберугроз.

2) Умные города:

В сфере "умных городов" женщины вносят свой вклад в разработку и внедрение безопасных технологий. Анджана Раджан, специалист по правам человека, является одним из таких примеров, работая над безопасными решениями для "умного города", которые интегрируют меры безопасности для защиты взаимосвязанных систем. Женщины в этой области предлагают уникальные перспективы, которые помогают удовлетворить разнообразные потребности городской среды в области безопасности, обеспечивая устойчивость инфраструктуры "умного города" к угрозам.

- **Анджана Раджан** - работает над безопасными решениями для умного города, интегрируя меры кибербезопасности для защиты взаимосвязанных городских систем.
- **Айя Бдейр** - основатель littleBits, библиотеки электронных модулей с открытым исходным кодом, которая позволяет любому создавать прототипы и решения для умных городов.
- **Воздействие**: Повышение устойчивости городской инфраструктуры к киберугрозам с помощью инновационных мер кибербезопасности.

3) Железнодорожная отрасль:

В железнодорожной отрасли растёт число женщин, вносящих свой вклад в обеспечение кибербезопасности. Марта, менеджер по техническим вопросам UNIFE, специализируется на исследованиях, инновациях и кибербезопасности в железнодорожном секторе. её работа включает разработку стратегий защиты железнодорожных систем от киберугроз, обеспечивающих безопасность и надёжность железнодорожного транспорта.

- **Мэри Уолтон** - Разработала первого промышленного робота, Unimate, который использовался в автомобилестроении, а позже был адаптирован для обслуживания железных дорог.
- **Ольга Трофимова** - Разработала первую автоматизированную систему управления ЖД, которая повысила безопасность и эффективность работы железных дорог.
- **Воздействие**: Разработка стратегий защиты железнодорожных систем, обеспечение безопасности и надёжности железнодорожного транспорта.

4) Фармацевтика/Биотехнологии:

В фармацевтической и биотехнологической промышленности женщины играют решающую роль в обеспечении безопасности конфиденциальных медицинских данных и научных исследований. Например, меры безопасности в этих отраслях жизненно важны для защиты интеллектуальной собственности и информации о пациентах от киберугроз. Женщины, занимающие должности в сфере кибербезопасности в этих секторах, участвуют в разработке и внедрении надёжных протоколов безопасности для защиты критически важных данных и обеспечения соответствия нормативным стандартам.

- **Каталин Карико** - её работа над технологией мРНК заложила основу для разработки мРНК-вакцин, включая вакцины Pfizer-BioNTech и Moderna против COVID-19.
- **Tu Youyou** - открыла артемизинин, препарат, используемый для лечения малярии, за что была удостоена нобелевской премии по физиологии и медицине в 2015 году.
- **Влияние**: Внедрение надёжных протоколов безопасности для защиты интеллектуальной собственности и информации о пациентах.

5) Кибербезопасность:

Кибербезопасность — это развивающаяся область, которая сочетает кибербезопасность с биологическими исследованиями и биотехнологиями. Женщины находятся на передовой этой области, решая уникальные проблемы безопасности, возникающие в результате интеграции цифровых и биологических систем. Их вклад включает разработку стратегий защиты биоинформационных данных, обеспечение безопасности процессов биомоделирования и обеспечение целостности биологических исследований от киберугроз. Женщины в области кибербезопасности внедряют инновации и устанавливают стандарты для обеспечения пересечения биологии и технологий.

- **Меган Палмер** - пионер в области безопасности, она внесла свой вклад в разработку стратегий защиты биоинформационных данных и биологических исследований от киберугроз.
- **Диана Дьюлис** - её работа сосредоточена на обеспечении безопасности процессов биомоделирования и обеспечении целостности биологических продуктов от киберугроз.
- **Воздействие**: Защита биоинформационных данных и процессов биомоделирования, обеспечение целостности биологических исследований.

III. Инклюзивность в кибербезопасности

A. Как подходы женщин отличаются от традиционных стратегий кибербезопасности

Подходы, которыми руководствуются женщины в сфере кибербезопасности, часто отличаются от традиционных стратегий по нескольким ключевым направлениям,

подчёркивая инклюзивность, ориентированный на человека дизайн и интеграцию различных точек зрения

- **Человекоцентричный и инклюзивный подходы:** Женщины в сфере кибербезопасности часто выступают за человекоцентричный подход к кибербезопасности. Это предполагает учёт потребностей и опыта всех пользователей, особенно маргинализированных групп, и обеспечение того, чтобы меры кибербезопасности были инклюзивными и справедливыми. Например, в отчёте Hofstetter и Pourmalek подчёркивается важность учёта опыта женщин и знаний женских правозащитных организаций в политике кибербезопасности".

- **Разработка и политики, учитывающие гендерные аспекты:** Женщины в сфере кибербезопасности настаивают на разработке технологий и политик, учитывающих гендерные аспекты. Это включает в себя рассмотрение гендерных последствий систем, процессов и практик кибербезопасности. В отчёте Фонда ICT4Peace подчёркивается, что при разработке технологий часто неправильно понимается или не учитывается гендерное использование, что создаёт дополнительные трудности в плане безопасности для женщин и других маргинализированных групп.

- **Разнообразие и вовлеченность в команды:** Женщины-лидеры в области кибербезопасности подчёркивают важность разнообразия и вовлеченности в команды, что считается более эффективным в реагировании на широкий спектр киберугроз из-за их различных точек зрения и опыта. Например, в отчёте Check Point Software отмечается, что команды с различным гендерным разнообразием в 73% случаев принимают лучшие бизнес-решения и более творчески подходят к решению проблем. Такой акцент на разнообразии контрастирует с традиционными командами по кибербезопасности

- **Обращение к гендерным нормам и стереотипам:** Чарли Дэвис из Sapphire подчёркивает необходимость упреждающих стратегий для привлечения разнообразных талантов и расширения возможностей наставничества для женщин в сфере кибербезопасности. Этот подход направлен на устранение барьеров и создание более инклюзивной среды, отличающейся от традиционных стратегий, которые могут прямо не затрагивать эти проблемы.

- **Этичное и ответственное использование ИИ:** Мурати из OpenAI выступает за регулирование искусственного интеллекта и общественное тестирование, чтобы привести технологии искусственного интеллекта в соответствие с намерениями человека и позитивно послужить человечеству. Такой акцент на этических соображениях и подотчётности общественности является отходом от традиционных стратегий кибербезопасности, которые могут отдавать приоритет техническим решениям, а не этическим последствиям.

- **Целостные стратегии защиты на основе сотрудничества:** Женщины, занимающиеся кибербезопасностью, часто продвигают целостные стратегии защиты на основе сотрудничества. Это включает в себя интеграцию искусственного интеллекта и машинного обучения для усиления мер безопасности и опережения возникающих угроз.

B. Гендерное влияние на понимание кибербезопасности

Гендерные нормы играют решающую роль в формировании понимания кибербезопасности, влияя на восприятие, поведение и выбор профессии.

- **Влияние гендерных норм на восприятие и поведение:** Гендерные нормы формируют индивидуальную идентичность, роли и ожидания в рамках кибербезопасности и общества в целом. Эти нормы часто ассоциируют технические знания с мужчинами и маскулинностью, в то время как знания в области коммуникаций или инициативы по обеспечению равенства связаны с женщинами и женственностью. Такая иерархическая социальная структура может привести к недооценке вклада, обычно связанного с женщинами, что влияет на то, как молодые люди воспринимают кибербезопасность и взаимодействуют с ней.

- **Гендерный опыт и осведомлённость в области кибербезопасности:** Исследования показывают, что гендерный фактор влияет на осведомлённость и поведение в области кибербезопасности. Например, исследование, проведённое среди тайских служащих, показало, что сотрудницы имеют более высокий уровень осведомлённости о кибербезопасности, чем их коллеги-мужчины. Это говорит о том, что гендерные нормы и процессы социализации могут влиять на то, как представители разных полов подходят к кибербезопасности и расставляют приоритеты в ней.

- **Социокультурные факторы и политические последствия**: Исследование, сравнивающее представления о кибербезопасности в Турции и Италии, подчёркивает, что эти социокультурные факторы, включая гендерные нормы, существенно влияют на понимание кибербезопасности молодыми людьми. Эти нормы влияют на то, как молодые люди воспринимают киберугрозы, на их чувство безопасности и на их реакцию на киберугрозы. В исследовании подчёркивается необходимость политики кибербезопасности, учитывающей гендерные аспекты и учитывающей эту социокультурную динамику, для эффективного решения проблем кибербезопасности.

- **Системы кибербезопасности с учётом гендерных факторов**: для учёта гендерных аспектов кибербезопасности важно внедрять системы

кибербезопасности с учётом гендерных факторов, учитывающие различный опыт и потребности представителей всех полов. Это включает в себя учёт гендерной проблематики при внедрении кибернорм, обеспечение наращивания потенциала с учётом гендерных факторов и устранение гендерного цифрового разрыва. Такие подходы гарантируют, что меры кибербезопасности будут всеобъемлющими и эффективными для всех, независимо от пола.

C. Проблемы, связанные с включением гендерных аспектов в стандарты кибербезопасности

Интеграция гендерных аспектов в стандарты кибербезопасности сталкивается с рядом проблем:

- **Отсутствие данных с разбивкой по полу:** существует значительный пробел в данных с разбивкой по полу, что имеет решающее значение для понимания конкретных потребностей в кибербезопасности и уязвимости различных гендерных идентичностей. Такой недостаток данных затрудняет разработку целенаправленных и эффективных политик и стандартов безопасности.
- **Недопредставленность женщин и гендерных меньшинств:** Женщины и гендерные меньшинства недопредставлены в управлении безопасностью и процессах принятия решений. Такая недопредставленность означает, что их точки зрения и опыт часто не учитываются, что приводит к разработке политики и стандартов, которые могут не соответствовать их конкретным потребностям.
- **Гендерные иерархии и предубеждения:** Практики и стандарты кибербезопасности часто отражают гендерные иерархии и предубеждения, отдавая приоритет техническому опыту по сравнению с другими формами знаний и участия.
- **Недостаточный учёт гендерной проблематики**: Во многих существующих стандартах и рамках кибербезопасности отсутствует системный подход к учёту гендерных аспектов. Это означает, что гендерные аспекты не всегда учитываются при разработке, внедрении и оценке мер безопасности, что приводит к неспособности учитывать гендерные аспекты угроз и практики кибербезопасности
- **Сопротивление изменениям и недостаточная осведомлённость:** возникает сопротивление включению гендерных соображений в стандарты безопасности из-за недостаточной осведомлённости или понимания значимости гендера для кибербезопасности. Некоторые заинтересованные стороны могут рассматривать гендерную проблематику скорее как второстепенный вопрос, чем как центральный компонент эффективного управления кибербезопасностью.
- **Сложность интерсекциональности:** Вопрос гендера в кибербезопасности требует интерсекционального подхода, который учитывает взаимосвязь гендера с другими факторами, такими как раса, класс, возраст, инвалидность и сексуальность. Такая сложность может затруднить разработку инклюзивных стандартов.

D. Основные гендерные последствия практики кибербезопасности

Гендерные последствия практики кибербезопасности многогранны и включают:

- **Дизайн и технология:**
  - Технологии безопасности часто наследуют гендерные предубеждения в процессах их разработки. Это может привести к появлению технологий, которые неадекватно защищают женщин и маргинализированные группы или возлагают на них дополнительное бремя.
  - Разработка с учётом гендерных факторов имеет решающее значение для обеспечения эффективности инструментов безопасности для всех пользователей, независимо от пола.
- **Защитные меры:**
  - Защитные методы кибербезопасности могут отражать мужские нормы, такие как акцент на техническую компетентность и автономию. Это может затруднить людям обращение за помощью или признание своей уязвимости, особенно в среде, где доминируют мужчины.
  - Гендерные нормы, касающиеся уязвимости и сотрудничества, могут препятствовать эффективной защите кибербезопасности, поскольку отдельные лица могут неохотно работать совместно или прозрачно.
- **Реагирование на инцидент:**
  - Гендерная динамика может влиять на состав и культуру групп реагирования на инциденты. Команды, которым не хватает разнообразия, менее эффективными в противодействии всему спектру киберугроз и могут увековечивать гендерные предубеждения в своих действиях.
  - Неформальные сети и сообщества кибербезопасности, основанные на доверии, могут исключать женщин и маргинальные группы, уменьшая их участие и влияние в усилиях по реагированию на инциденты.

E. Гендерные модели угроз

1) Гендерные модели угроз влияют на стратегии безопасности

Гендерные модели угроз существенно влияют на стратегии кибербезопасности, формируя то, как угрозы воспринимаются, расставляются по приоритетам и устраняются.

- **Различное восприятие угрозы:**

- Гендерные модели угроз часто отражают предубеждения общества, что приводит к недопредставленности или искажению угроз, которые непропорционально сильно затрагивают женщин и маргинализированные группы. Например, онлайн-домогательства, киберпреследование и несанкционированный обмен интимными изображениями, скорее всего, будут преуменьшены или опущены в традиционных моделях угроз.
- Это может привести к тому, что стратегии кибербезопасности не будут должным образом защищать эти группы, делая их более уязвимыми к определенным типам киберугроз.

- **Дополнительные трудности с обеспечением безопасности:**
  - Женщины и маргинализированные группы могут столкнуться с дополнительными трудностями в плане безопасности из-за моделей гендерных угроз. Например, им может потребоваться принять более надёжные меры конфиденциальности или принять дополнительные меры предосторожности для защиты своих учётных данных в Интернете, что может занять много времени и затратно.
  - Стратегии кибербезопасности, которые не учитывают эти дополнительные трудности, могут непреднамеренно усилить нагрузку на эти группы, снижая эффективность.

- **Неискренний маркетинг кибербезопасности:**
  - Гендерные модели угроз также могут влиять на маркетинг технологий безопасности. Реклама товаров может не соответствовать конкретным потребностям женщин и маргинализированных групп и не удовлетворять их, что приводит к снижению показателей усыновления среди этих групп населения.
  - Эффективные стратегии кибербезопасности должны включать маркетинговые подходы, которые являются инклюзивными и учитывают разнообразные потребности всех пользователей

2) Гендерные стереотипы влияют на моделирование угроз

Гендерные стереотипы играют важную роль в формировании моделей угроз кибербезопасности, влияя как на разработку, так и на выполнение этих упражнений:

- **Стереотипные характеристики:**
  - Моделирование угроз часто связано с гендерными стереотипами, когда роли и сценарии основаны на традиционных гендерных нормах. Например, мужчины могут быть изображены в качестве основных защитников или нападающих, в то время как женщины изображаются в менее технических или вспомогательных ролях.
  - Это может усилить гендерные предубеждения и ограничить предполагаемые возможности женщин и других маргинализованных групп в области кибербезопасности.

- **Нормы маскулинности в обороне:**
  - Концепция защиты в сфере кибербезопасности часто ассоциируется с нормами маскулинности, такими как техническая компетентность, автономия и защита. Эти нормы могут затруднить людям признание ошибок, обращение за помощью или совместную работу, которые необходимы для эффективной защиты в сфере кибербезопасности.
  - Гендерные нормы, касающиеся уязвимости, могут препятствовать прозрачности и сотрудничеству, что приводит к менее эффективному моделированию угроз и реагированию в реальном мире.

3) Гендерные модели угроз. Сценарии фишинга

Гендерные модели угроз могут существенно влиять на подход к моделированию фишинга, приводя к различиям в том, как эти модели разрабатываются, выполняются и оцениваются.

- **Определение приоритетности угроз:**
  - В традиционных моделях угроз приоритет часто отдаётся фишинговым атакам, нацеленным на финансовые или корпоративные данные, которые могут не учитывать угрозы, с которыми чаще сталкиваются женщины и маргинальные группы, такие как онлайн-домогательства, киберпреследование и несанкционированный обмен интимными изображениями.
  - Моделирование фишинга на основе этих традиционных моделей может не соответствовать адекватно конкретной тактике социальной инженерии, используемой при киберугрозах по признаку пола.

- **Разработка сценария:**
  - Фишинговые симуляции часто включают гендерные стереотипы в изображаемых ролях и сценариях, укрепляя традиционные гендерные нормы.
  - Мужчины могут быть изображены как основные защитники или нападающие, в то время как женщины изображены в менее технических или вспомогательных ролях.
  - Такие стереотипные характеристики могут усиливать гендерные предубеждения и ограничивать предполагаемые возможности женщин и других маргинализованных групп в области кибербезопасности.

- **Отбор участников:**
  - На состав участников симуляций фишинга может влиять гендерная динамика, что потенциально приводит к недопредставленности женщин и маргинализированных групп.
  - Это может привести к моделированию, которое не сможет отразить разнообразный опыт и уязвимость, с которыми сталкиваются представители разных гендерных идентичностей.
- **Показатели оценки:**
  - При традиционном моделировании фишинга успех часто оценивается на основе таких показателей, как количество переходов или утечка данных, которые могут неадекватно отражать влияние киберугроз по признаку пола.
  - Модели гендерных угроз могут требовать различных показателей оценки, учитывающих психологические и социальные последствия фишинговых атак для различных гендерных идентичностей.
- **Защитные стратегии:**
  - Защитные стратегии, которым обучают при моделировании фишинга, могут отражать мужские нормы, такие как акцент на техническую компетентность и автономию.
  - Это может затруднить обращение за помощью, признание уязвимостей или совместную работу, что необходимо для эффективной защиты в сфере кибербезопасности.
- **Реагирование на инцидент:**
  - Гендерная динамика может влиять на состав и культуру групп реагирования на инциденты, участвующих в моделировании фишинга.
  - Команды, которым не хватает разнообразия, могут быть менее эффективными в противодействии всему спектру киберугроз и могут увековечивать гендерные предубеждения в своих действиях

Для решения этих проблем крайне важно учитывать гендерные аспекты при моделировании фишинга.

- Разработка моделей угроз, учитывающих уникальные уязвимости и опыт различных гендерных идентичностей.
- Обеспечение разнообразного и инклюзивного отбора участников и разработки сценария.
- Оценка симуляций на основе показателей, отражающих психологические и социальные последствия киберугроз по признаку пола.
- Продвижение защитных стратегий, подчёркивающих сотрудничество, прозрачность и стремление к поддержке.
- Содействие разнообразию и инклюзивности в группах реагирования на инциденты, участвующих в моделировании фишинга.

4) Лучшие практики обучения кибербезопасности с учётом гендерных факторов

Для решения этих проблем и создания более инклюзивных стратегий кибербезопасности рекомендуются следующие передовые методы обучения кибербезопасности с учётом гендерных факторов:

- **Разработка инклюзивной учебной программы:** учебные материалы, посвящённые конкретным угрозам безопасности, с которыми сталкиваются представители различных гендерных идентичностей, включая тематические исследования и сценарии, отражающие разнообразный гендерный опыт.
- **Моделирование угроз с учётом гендерных факторов:** моделирование угроз с учётом гендерных факторов в учебные программы, включая уникальные уязвимости и потребности в безопасности всех гендерных групп.
- **Поощрять разнообразие и инклюзивность:** участие женщин и маргинализированных групп в учебных программах по безопасности, включая инклюзивную среду обучения, в которой ценятся разнообразные точки зрения и опыт.
- **Устранение гендерных предубеждений и стереотипов:** обучение по распознаванию и устранению гендерных предубеждений и стереотипов в практике обеспечения безопасности, в т.ч. вызов традиционным нормам и продвижение культуры прозрачности и сотрудничества.
- **Сотрудничать с гражданским обществом и научными кругами:** Работа с организациями гражданского общества и академическими институтами над разработкой комплексных и межсекторальных учебных программ по кибербезопасности. Такое сотрудничество может помочь обеспечить, чтобы учебные материалы основывались на последних исследованиях и передовой практике в области кибербезопасности с учётом гендерных факторов.
- **Непрерывный мониторинг и оценка:** механизмы непрерывного мониторинга и оценки учебных программ по безопасности, чтобы гарантировать, что они остаются всеобъемлющими и эффективными, включая отзывы участников и вносите необходимые коррективы для устранения любых пробелов или предвзятостей.