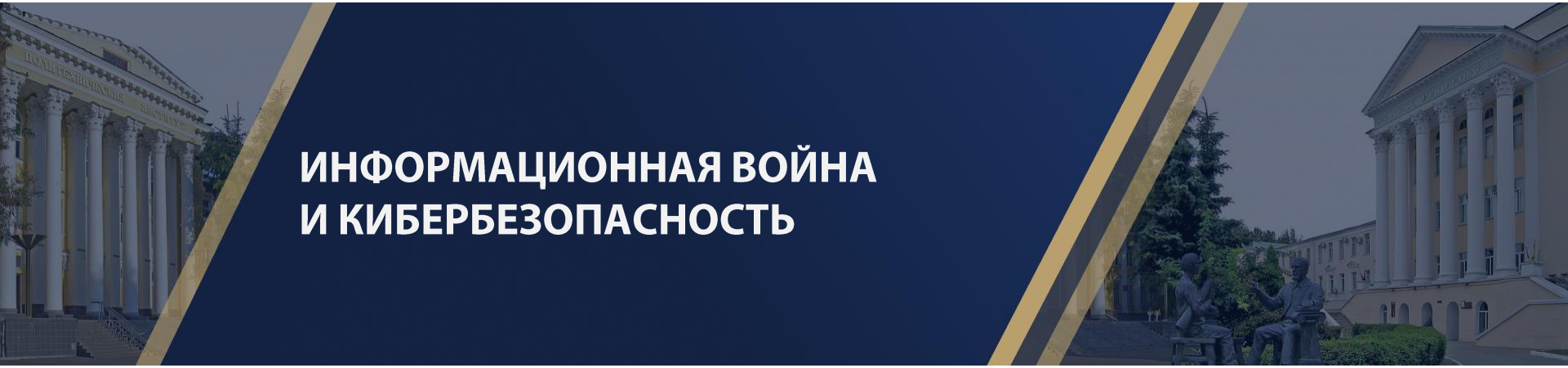
ВГТУ

**ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**РЕГИОНАЛЬНЫЙ УЧЕБНО-НАУЧНЫЙ ЦЕНТР ПО ПРОБЛЕМАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**



# ИНФОРМАЦИОННАЯ ВОЙНА И КИБЕРБЕЗОПАСНОСТЬ

**ОСТАПЕНКО АЛЕКСАНДР ГРИГОРЬЕВИЧ**
Заведующий кафедрой систем информационной безопасности,
доктор технических наук, профессор

# ГЛОССАРИЙ

**УГРОЗА**
Совокупность факторов, влияние которых способно нанести ущерб защищаемой системе

**РИСК**
Возможность наступления ущерба

**БЕЗОПАСНОСТЬ**
Состояние системы, при котором риск реализации угроз не превышает допустимых значений

**ИНЦИДЕНТ**
Зарегистрированное событие нарушения безопасности системы

**АТАКА**
Кратковременное решительное деструктивное воздействие злоумышленника, нацеленное на нарушение безопасности системы

**ОПЕРАЦИЯ**
Скоординированная злоумышленником последовательность атак на систему

# ГЛОССАРИЙ

**ИНФОРМАЦИОННАЯ ВОЙНА**
Противоборство государств в глобальном информационном пространстве посредством реализации психологических и кибернетических операций

**ГИБРИДНАЯ ВОЙНА**
Вид враждебных действий противоборствующих сторон, при котором исключено военное вторжение, а скрытно реализуются операции экономического, информационного и прочего характера

**МЕНТАЛЬНАЯ ВОЙНА**
Скоординированная совокупность информационных операций, направленных на «оккупацию» сознания противника в целях паралича его воли, изменения индивидуального и массового сознания населения

# 1 КИБЕРДРУЖИНА

1. Организована по **инициативе ректора ВГТУ Д. К. Проскурина** и вот уже более семи лет активно участвует в защите отечественного информационного пространства от психологических и кибернетических атак:
   - выявляя и обезвреживая деструктивные контенты;
   - обнаруживая и ликвидируя последствия компьютерных атак.
2. Сегодня студенты и аспиранты, входящие в состав кибердружины, решают вышеперечисленные задачи уже при помощи **средств искусственного интеллекта**, приобретая самые современные компетенции в области ИБ.
3. Нейросетевые технологии применяются кибедружинниками при:
   - визуализации и популяризации перспективных направлений защиты информации среди абитуриентов и младшекурсников;
   - подготовке специалистов по защите информации и профессиональной проектной деятельности путём создания конкурентноспособных продуктов;
   - выполнении специальных задач по обеспечению национальной безопасности.
4. Мы открыты и готовы для взаимодействия с физическими лицами и структурами, заинтересованными в защите интересов России в информационной среде (**Narhov.dima@mail.ru**).

# 2 ДЕСТРУКТИВНЫЕ ИДЕОЛОГЕМЫ ЗАПАДА

1. Сегодня количество адептов деструктивных идеологем (ЛГБТ, Чайлд-Фри, безбожие, неонацизм и др.) измеряется двузначными процентами.
   Они уже **не маргиналы** и **пользуются поддержкой** власти.
2. Эта скверна проникает и в наше общество, в связи с чем в России законодательно запрещена пропаганда **ЛГБТ** и **«Чайлд-Фри»**.
3. Однако, борьба с этими движениями недостаточно эффективная из-за того, что:
   - **прозападные соцсети и мессенджеры** по-прежнему оказывают существенное влияние на формирование общественного сознания;
   - **отечественная система воспитания** и образования довольно вяло осуждает адептов вышеперечисленных идеологем;
   - **регистрация, реагирование и ликвидация последствий** в отношении инцидентов, спровоцированных перечисленными идеологемами, оставляют желать в обществе и государстве много лучшего как по оперативности, так и по решительности мер противодействия.
4. Без устранения этих недостатков мы довольно быстро увидим, как эти маргиналы станут модными и начнут **разрушать Россию** изнутри.

# 3 ТЕХНОЛОГИИ КИБЕРМОШЕННИЧЕСТВА

## Масштабы ущерба от кибермошенничества

Современные технологии сделали кибермошенничество глобальной проблемой. По данным международных отчётов, ежегодные убытки от киберпреступности достигают триллионов долларов, затрагивая государство, бизнес и граждан.
В России ежеквартально фиксируется рост числа атак, включая утечку персональных данных и массовое финансовое мошенничество.

## Популярные технологии кибермошенников

Используются фишинг, социальная инженерия, вредоносное ПО, поддельные сайты и взлом аккаунтов. Преступники применяют технологии Deepfake и ИИ для создания убедительных подделок. Технологии становятся всё сложнее, делая распознавание мошенничества все труднее.

## Факторы, усложняющие борьбу

Анонимность в сети, использование криптовалют и распространение знаний о взломах в Даркнете затрудняют выявление мошенников. Часто жертвы сами способствуют мошенничеству, пренебрегая цифровой гигиеной.

## Эффективные меры противодействия

Ключевые шаги: массовое обучение пользователей, развитие культуры информационной гигиены, внедрение ИИ для мониторинга подозрительной активности. Только системный подход обеспечит снижение рисков.

# 4 КИБЕРАТАКИ

## Масштабы ущербов

Кибератаки ежегодно наносят ущерб на триллионы долларов, затрагивая бизнес, государственные системы и пользователей, вызывая утечку данных и сбои в инфраструктуре.

## Популярные виды атак

Наиболее распространены фишинг, DDoS-атаки, инъекции вредоносного ПО и взломы через цепочки поставок. Активно используются методы социальной инженерии и технологии искусственного интеллекта.

## Основные противодействующие силы

Борьбой с угрозами занимаются государственные центры реагирования ГосСОПКА, IT-компании и разработчики решений по защите инфраструктур, - работодатели для наших выпускников.

## Эффективные технологии защиты

Эффективные меры включают машинное обучение, поведенческий анализ, шифрование данных и автоматизированные системы мониторинга для быстрого обнаружения и нейтрализации атак.

# 5 ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК УГРОЗА

## Рост угроз со стороны ИИ

Искусственный интеллект становится мощным инструментом для кибератак и деструктивной деятельности. Автоматизация взломов, создание фейковых данных и реалистных подделок (Deepfake) увеличивают разнообразие и сложность угроз.

## Манипуляция информацией

ИИ активно используется для создания фейков, манипулирования общественным мнением и распространения дезинформации в масштабах, ранее недоступных человеку. Это подрывает доверие к информации и государственным институтам.

## Оружие для киберпреступников

ИИ помогает мошенникам автоматизировать атаки: от взлома паролей и систем до создания персонализированных фишинговых сообщений. Алгоритмы предсказывают поведение жертв и обходят традиционные системы защиты.

## Пробелы в противодействии

Существующие методы защиты часто не успевают за развитием ИИ. Необходимо создавать этичные и регулируемые системы ИИ, внедрять алгоритмы противодействия и повышать готовность к новым угрозам.

# 6 ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ВОЗМОЖНОСТЬ

**Обнаружение и предотвращение угроз**
ИИ позволяет анализировать большие объемы данных в реальном времени, выявляя аномалии и подозрительную активность. Машинное обучение помогает предсказывать атаки до их совершения, значительно сокращая время реакции на угрозы.

**Автоматизация мониторинга и реагирования**
Системы ИИ автоматически обрабатывают инциденты, классифицируют угрозы и принимают меры для нейтрализации атак. Это снижает зависимость от человека и повышает эффективность защиты.

**Улучшение анализа уязвимостей**
ИИ помогает сканировать сети и системы на наличие уязвимостей, анализировать поведение пользователей и выявлять потенциальные слабые места до того, как они будут использованы злоумышленниками.

**Борьба с фишингом и мошенничеством**
Системы на основе ИИ распознают фишинговые письма, поддельные сайты и мошеннические транзакции с высокой точностью, защищая пользователей от обмана и последующей кражи данных.

# 7 КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

## Угроза традиционному шифрованию

Квантовые компьютеры способны взламывать традиционные криптографические алгоритмы. Это ставит под угрозу конфиденциальность данных и безопасность систем, основанных на классическом шифровании.

## Разработка квантоустойчивой криптографии

В ответ на угрозу разрабатываются квантоустойчивые алгоритмы шифрования, устойчивые к атакам квантовых компьютеров. Их внедрение необходимо для защиты данных в долгосрочной перспективе.

## Ускорение атак и аналитики

Квантовые вычисления могут значительно ускорить выполнение задач по подбору паролей и взлому систем, а также обработку больших массивов данных, что создаёт новые риски для информационной безопасности.

## Новые возможности для защиты

Квантовые технологии также предлагают новые методы защиты, такие как квантовая криптография и квантовое распределение ключей (QKD), обеспечивающие максимально высокий уровень безопасности при передаче данных.

# 8 ОПЫТ КИТАЯ

## Жесткий контроль над интернет-пространством

Китай активно регулирует интернет с помощью «Великого китайского файрвола», который блокирует нежелательные ресурсы, контролирует контент и ограничивает влияние иностранных информационных угроз на население.

## Развитие собственных технологий

Китай инвестирует в создание национальных платформ и альтернативных сервисов (WeChat, Baidu, AliPay), уменьшая зависимость от западных технологических гигантов и минимизируя уязвимости и угрозы в цифровой среде.

## Государственная стратегия и социальный рейтинг

Китай реализует мощные программы по обеспечению ИБ, включая систему социального рейтинга, которая контролирует поведение граждан и организаций. Стратегия предусматривает централизованный мониторинг и защиту ключевых государственных и окологосударственных информационных систем.

## Технологии на основе ИИ и анализа больших данных

Китайские системы используют искусственный интеллект и анализ больших данных для выявления и предотвращения угроз. Эти технологии обеспечивают эффективный мониторинг, контроль и парирование информационных атак.


HEDRA