Угрозы информационной безопасности

Информационные войны

Оксана Докучаева

Проверка связи

Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти

Поставьте в чат:

\+ если меня видно и слышно

– если нет

Оксана Докучаева

О спикере:

- 13 лет оперативного опыта в Центре информационной безопасности ФСБ России
- Автор публикаций по информационной безопасности и расследованию компьютерных преступлений
- Опыт взаимодействия с Советом Безопасности РФ, правоохранительными органами, спецслужбами, организациями РФ и иностранных государств по вопросам обеспечения информационной безопасности

Правила участия

1. Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
2. Продолжительность вебинара — 80 минут
3. Вы можете писать свои вопросы в чате
4. Запись вебинара будет доступна в LMS

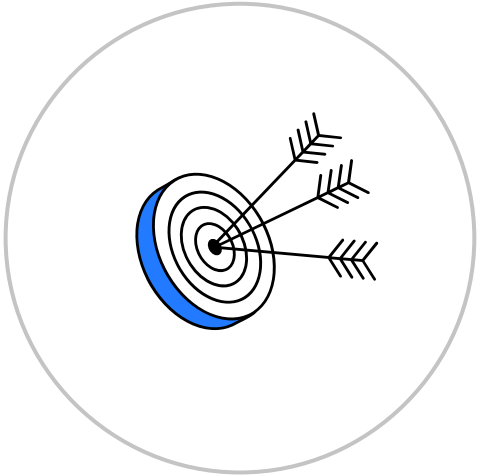
Зачем это специалисту по информационной безопасности?

Вспомним первую лекцию

1. Узнали пути возникновения и становления отрасли информационной безопасности в современном мире
2. Разобрались с профессиональной терминологией, применяемой в отрасли
3. Разобрали задачи информационной безопасности на территории РФ — как частные, так и глобальные
4. Изучили базовые элементы информационной безопасности
5. Разобрали концептуальные основы информационной безопасности на уровне государства и организаций

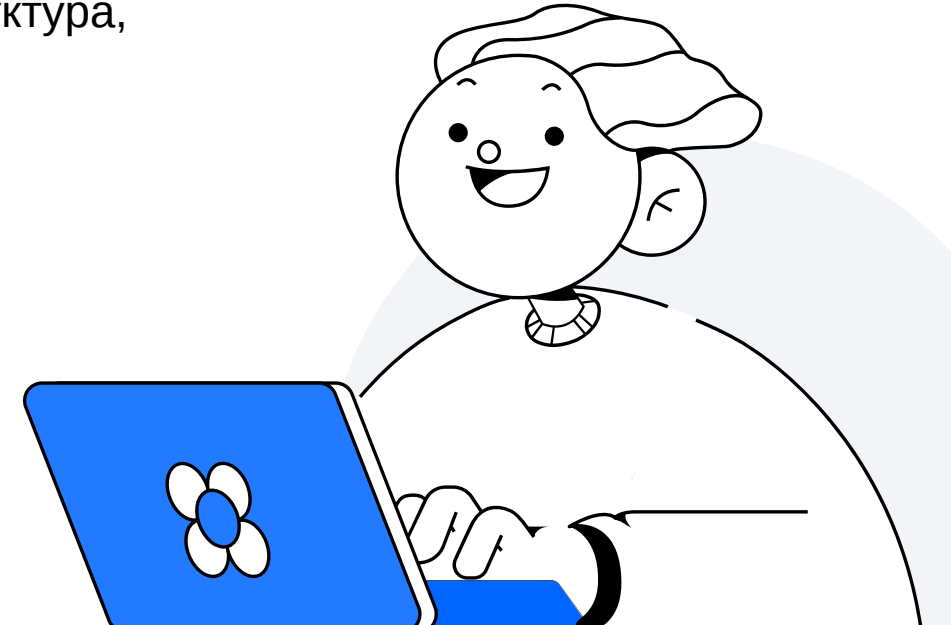
Цели занятия

- Узнаем, какие угрозы информационной безопасности страны возможны, изучим источники угроз
- Узнаем, что такое информационные войны
- Рассмотрим виды информационных войн
- Обсудим яркие примеры современных информационных войн



План занятия

1. Угрозы информационной безопасности страны и их источники
2. Информационные войны. Общие сведения
3. Информационные войны. Виды, структура, стратегии, оружие
4. Итоги занятия
5. Домашнее задание



Угрозы информационной безопасности и их источники

1

Угрозы информационной безопасности РФ

Совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Согласно Доктрине информационной безопасности Российской Федерации

Источник

Виды угроз

- Оборот информации в нарушение норм международного права
- Информационно-техническое воздействие
- Техническая разведка
- Информационно-психологическое воздействие
- Дискриминация СМИ
- Компьютерная преступность
- Компьютерные атаки
- Низкая конкурентоспособность собственных ИТ-технологий
- Высокая зависимость от зарубежных производителей
- Низкий уровень обеспечения ИБ
- Доминирование отдельных стран в сетевом пространстве
- Низкий уровень международной информационной безопасности

Приведите примеры угроз ИБ, с которыми вы встречаетесь в жизни

Оборот информации в нарушение норм международного права

Трансграничный оборот информации используют,
чтобы достичь противоречащих международному праву целей:

- геополитических
- военно-политических
- террористических
- экстремистских
- криминальных

Наносится ущерб международной безопасности
и стратегической стабильности

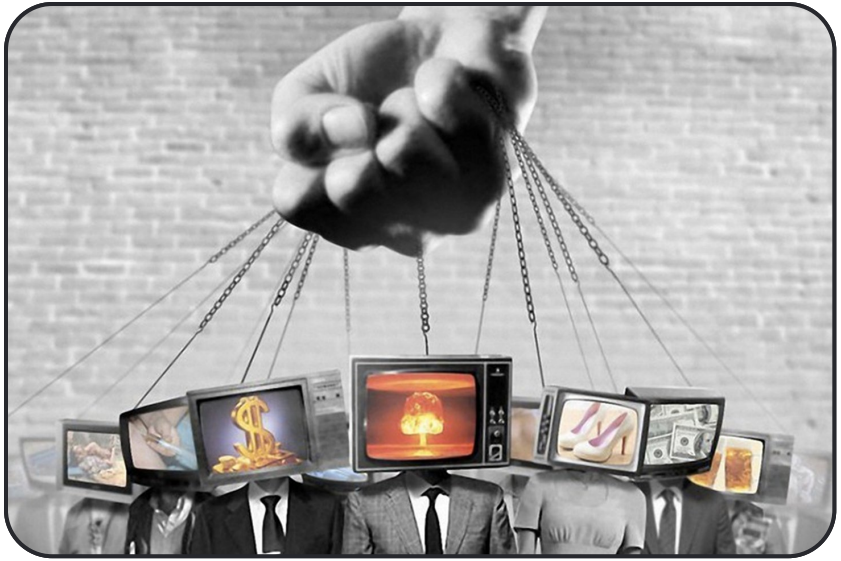
Информационно-техническое воздействие

Зарубежные страны оказывают информационно-техническое воздействие на информационную инфраструктуру в военных целях.

Отдельные государства и организации применяют информационные технологии в военно-политических целях.

Террористические и экстремистские организации создают средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Нарастает угроза применения информационных технологий с целью нанести ущерб суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации

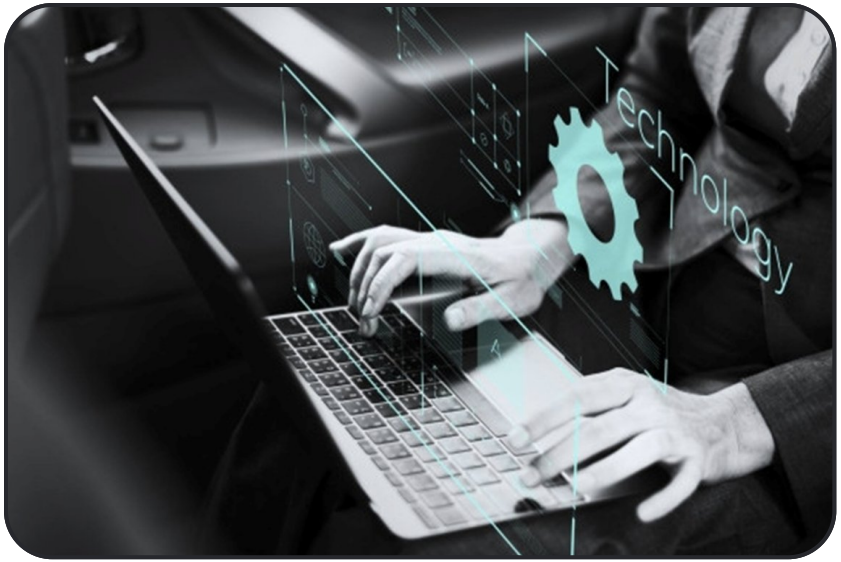


Источник

Техническая разведка

Усиливается деятельность организаций в отношении:

- российских государственных органов
- научных организаций
- предприятий оборонно-промышленного комплекса



Источник

Информационно-психологическое воздействие

Использование спецслужбами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира.

Информационное воздействие на население России с целью размыть традиционные российские духовно-нравственные ценности.

Информационное воздействие террористических и экстремистских организаций на индивидуальное, групповое и общественное сознание

Источник

Подумайте

Вы ощущали на себе информационно-психологическое воздействие?

Дискриминация СМИ

Генеральный прокурор РФ и его заместители наделены полномочиями по «запрету на территории РФ деятельности иностранного средства массовой информации при установлении факта принятия враждебных решений иностранными государствами в отношении российских СМИ, распространяемых за рубежом»

Источник

Компьютерная преступность

Рост компьютерной преступности:

- в кредитно-финансовой сфере
- в сфере неприкосновенности частной жизни
- в сфере личной тайны
- в сфере семейной тайны
- в сфере обработки персональных данных

Сталкивались ли вы или ваше окружение с компьютерными преступлениями?

Компьютерные атаки

- Постоянно повышается сложность
- Увеличивается масштаб и растёт скоординированность компьютерных атак на объекты критической информационной инфраструктуры
- Усиливается разведывательная деятельность иностранных государств в отношении Российской Федерации посредством совершения компьютерных атак

Источник

Низкая конкурентоспособность собственных ИТ-технологий

Недостаточный уровень развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг.

Недостаточная эффективность научных исследований в области информационных технологий.

Низкий уровень внедрения отечественных разработок

Источник

Высокая зависимость от зарубежных производителей

Высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части:

- электронной компонентной базы
- программного обеспечения
- вычислительной техники
- средств связи

Источник

Низкий уровень обеспечения ИБ

Низкая правовая культура в области обеспечения информационной безопасности.

Недостаточное кадровое обеспечение в области информационной безопасности.

Низкая осведомлённость граждан в вопросах обеспечения личной информационной безопасности

Источник

Доминирование отдельных стран в сетевом пространстве

Стремление отдельных государств использовать технологическое превосходство, чтобы доминировать в информационном пространстве.

Распределение между странами сетевых ресурсов не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими

Источник

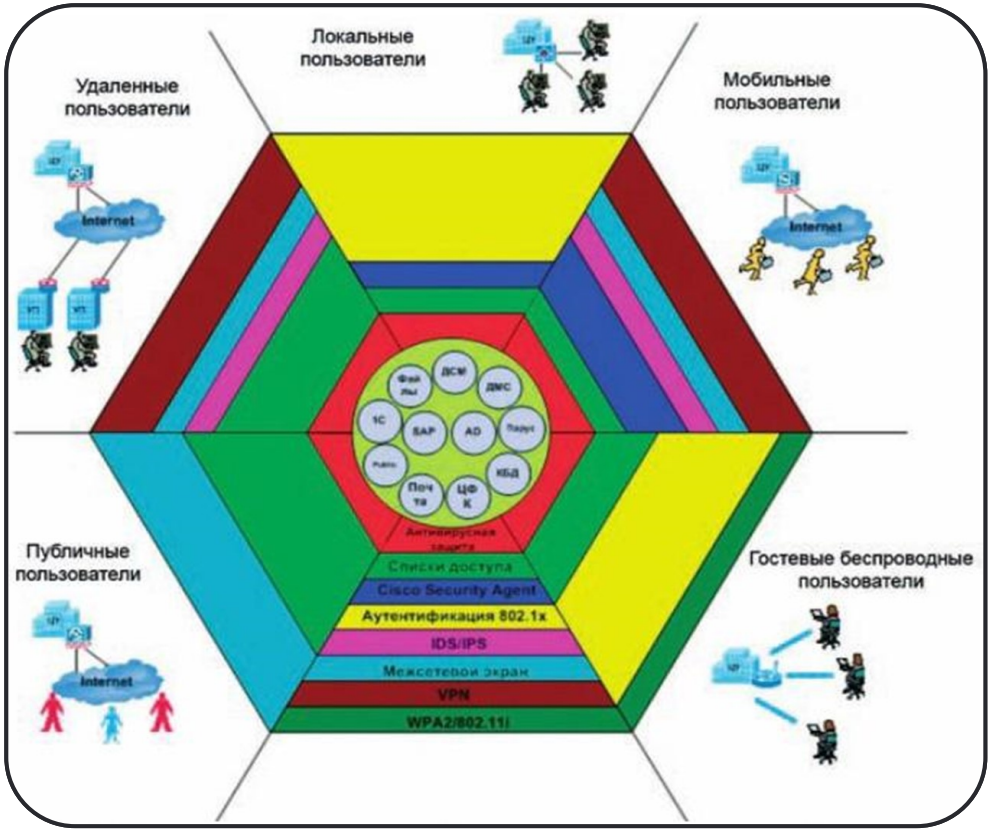
Низкий уровень международной информационной безопасности

Отсутствие:

- международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве
- механизмов и процедур их применения
- системы международной информационной безопасности

Источники угроз информационной безопасности

- Внешние
- Внутренние



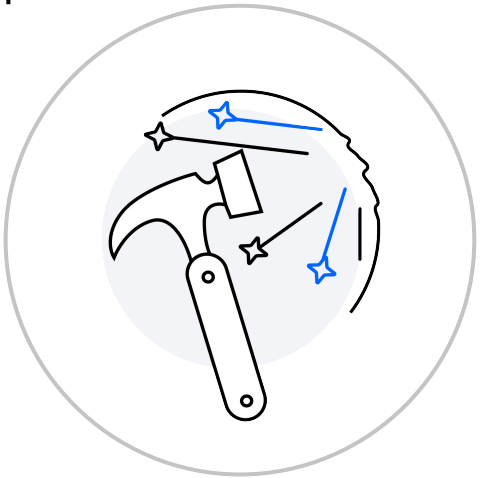
Источник

Внешние источники угроз

- Иностранные политические, экономические, военные, разведывательные, информационные структуры
- Международные террористические организации
- Международная конкуренция
- Технологический отрыв
- Разведка иностранных государств
- Информационные войны

Внутренние источники угроз

- Криминогенные структуры
- Террористические организации
- Недостаточная координация формирования и реализации единой госполитики в области обеспечения ИБ
- Несовершенство правовой базы и правоприменительной практики
- Недостаточное финансирование мероприятий по ИБ
- Неквалифицированные кадры
- Отставание в уровне информатизации



Выводы

1. Определение угрозам ИБ страны дано в Доктрине информационной безопасности
2. Существует несколько видов угроз ИБ
3. Угрозы ИБ связаны с разнообразными факторами
4. Источники угроз можно разделить на внешние и внутренние

Ваши вопросы

Информационные войны

Общие сведения

Информационная война (англ. information war) — противоборство сторон посредством распространения специально подготовленной информации и противодействия аналогичному внешнему воздействию на себя.

Википедия

Информационная война — процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня путём воздействия на гражданское население, власти и (или) вооружённые силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов и противодействия таким воздействиям на собственную сторону

А. В. Манойло

Информационные войны в древности

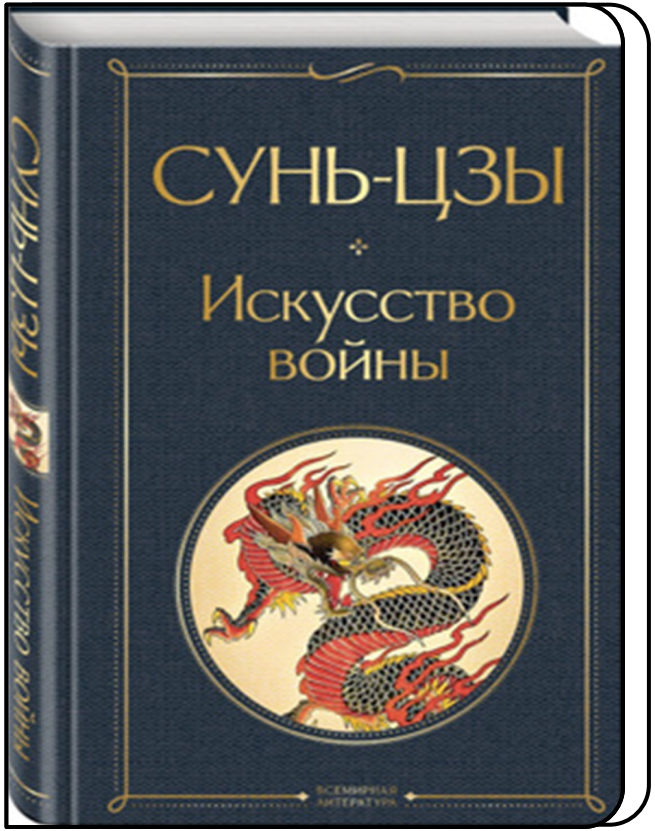
Форма — использование средств духовного воздействия для ослабления морального духа и боевой мощи противника, поднятие боевого духа своих войск

Основной носитель и средство доведения информации — человек

Объект воздействия — психика человека, сознание, воля и чувства

Способы вести информационное противоборство — вербальные технологии, наглядные средства устрашения и физического противодействия

Важнейшие субъекты — священнослужители как наиболее образованные люди, обладавшие значительным влиянием на все социальные слои



Источник

Информационные войны в Средние века

XIII в. — один из первых исторических примеров масштабного применения дезинформации в военных целях путём подделки указа о прекращении сопротивления.

Возросла роль религиозного фактора в ходе идейно-пропагандистского обеспечения крестовых походов для маскировки захватнических целей.

Велась отработка приёмов психологической войны — дискредитации противника путём распространения версии о зверствах, разжигания разногласий между государствами, обещания привилегий сдавшимся

Источник

Информационные войны XX века. Пропаганда

Возникновение интенсивной пропаганды для воздействия на массовое сознание и манипулирования им.

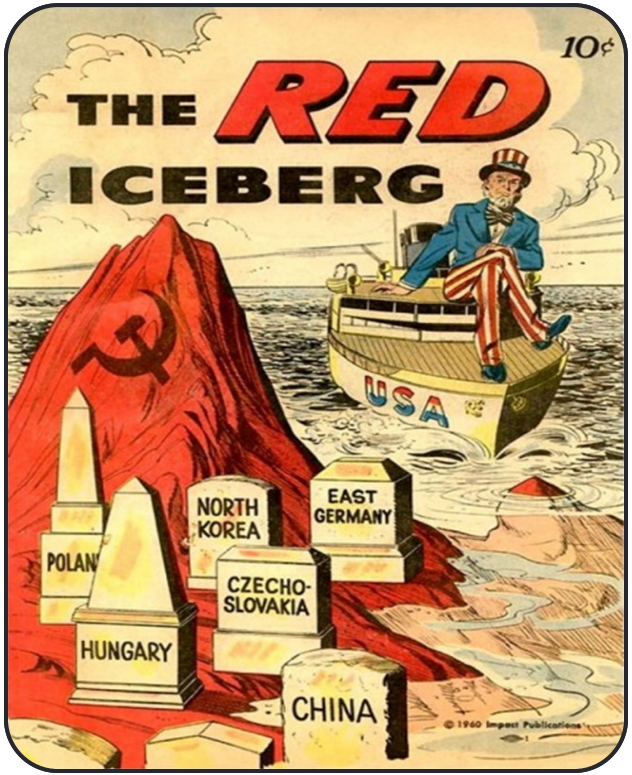
Цель пропаганды — поддерживать людей в нервном возбуждении.

Субъекты — государственные деятели и их окружение, подконтрольные государству СМИ.

Объекты — народные массы.

Позитивная пропаганда призвана способствовать социальной гармонии, согласию.

Негативная пропаганда предназначена для разжигания социальной вражды, эскалации социальных конфликтов, обострения противоречий в обществе



Источник

Информационные войны XXI века

Термин «информационная война» появился в 1976 году.

Сферы ведения информационного противоборства:

- политическая
- дипломатическая
- финансово-экономическая
- инновационная
- военная

Этапы информационных войн:

- оценка обстановки
- целеполагание
- определение замысла решения
- формирование вариантов решения (не менее трёх)

К концу XX – началу XXI века информационные войны получили развёрнутое теоретическое обоснование и стали изучаться как наука

Какие эпохи информационных войн кажутся вам наиболее интересными?

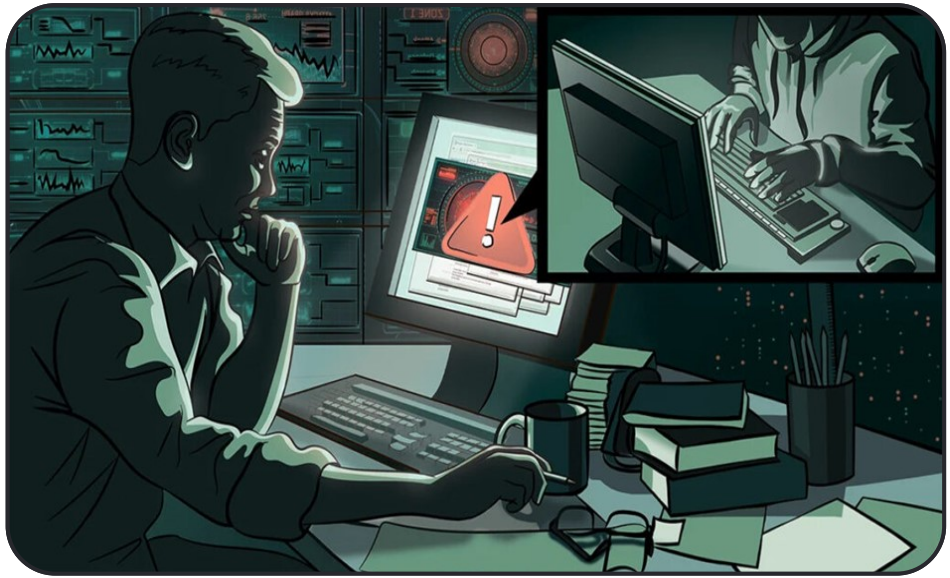
Элементы и уровни информационных войн

Три составных элемента информационных войн:

- стратегический анализ
- информационное воздействие
- информационное противодействие

Три уровня ведения информационных войн:

- стратегический
- оперативный
- тактический



Источник

Факторы информационных войн

- Наличие материально-технической базы
- Наличие финансовой базы
- Наличие высококвалифицированных специалистов
- Распределение кампании в пространстве и времени
- Доступ к СМИ

Источник

Выводы

1. Информационные войны существуют с древних времен
2. Радикальное изменение в тактике ведения информационных войн произошло в XX веке
3. В XXI веке сформировалась научно-теоретическая база по информационным войнам
4. Существуют различные элементы, уровни, факторы, цели информационных войн

Ваши вопросы

Информационные войны

Виды, структура, стратегии, оружие

3

Виды информационных войн по Мартину Либики

В августе 1995 года Мартин Либики (Национальный институт обороны США) опубликовал работу «Что такое информационная война?», определив **семь форм информационной войны:**

- командно-управленческая
- разведывательная война
- электронная война
- психологическая война
- хакерская война
- экономическая информационная война
- кибервойна
- семантические атаки

Источник

Виды информационных войн по Ю. П. Сурмину и Н. В. Туленкову

- Информационная агрессия
- Информационная экспансия
- Информационно-психологическая гражданская война

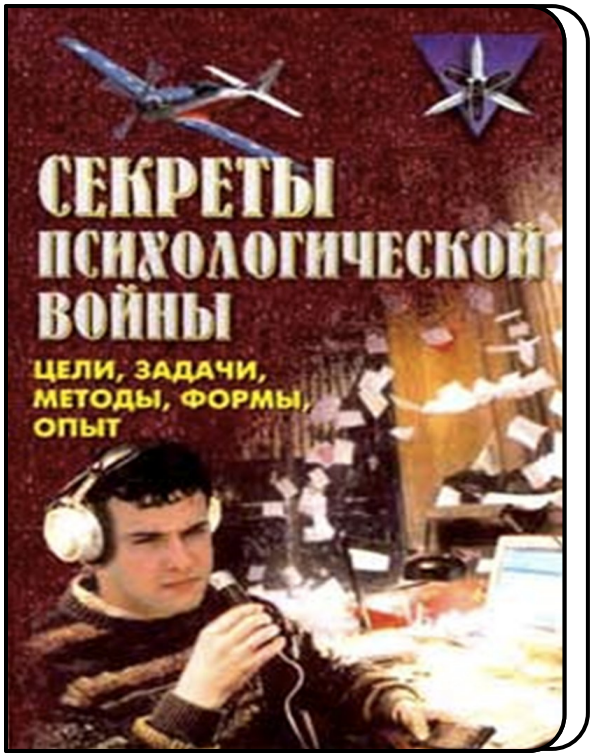
По предмету конфликта Ю. П. Сурмин и Н. В. Туленков выделяют следующие виды:

- психологическая война
- коммуникационная война
- информационная война
- ценностная или мировоззренческая война

Источник

Виды информационных операций по В. Г. Крысько

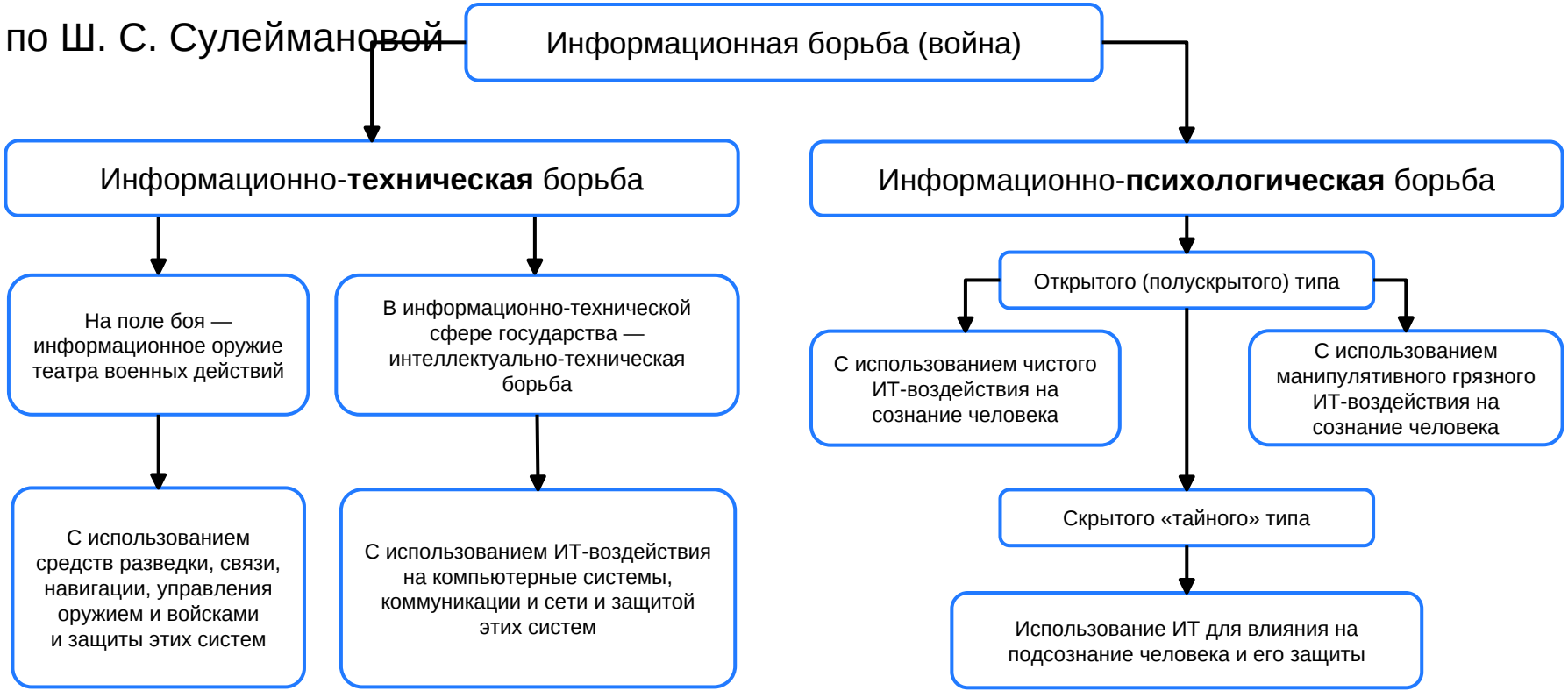
- Психологические операции
- Операции дезинформации
- Контрразведывательные операции
- Электронное противоборство
- Операции в компьютерных сетях



Источник

Структура современной информационной войны

по Ш. С. Сулеймановой



Стратегия информационной войны

- Изучить системы противника
- Определить цели обработки
- Подобрать входные данные, соответствующие цели
- В качестве цели представить собственные достоинства
- Организовать подачу материала, в т. ч. эмоционально заряженного
- Взаимодействовать с деятелями культуры и искусства противника, моделировать их поведение
- Привнести хаос в функционирование атакуемой системы
- Воздействовать на те элементы системы, которые поддаются обработке

Информационное оружие

Это средства уничтожения, искажения или хищения информации, дезорганизации работы технических средств, вывода из строя высокотехнологического обеспечения жизни общества и государства.

Источник

Особенности:

- скрытность
- масштабность
- универсальность

Объекты воздействия:

- сети связи государственных органов
- военная информационная инфраструктура
- информационные структуры банков, транспорта, промышленности
- СМИ

Подумайте

Если бы вы проводили информационную войну, с чего бы вы начали?

Выводы

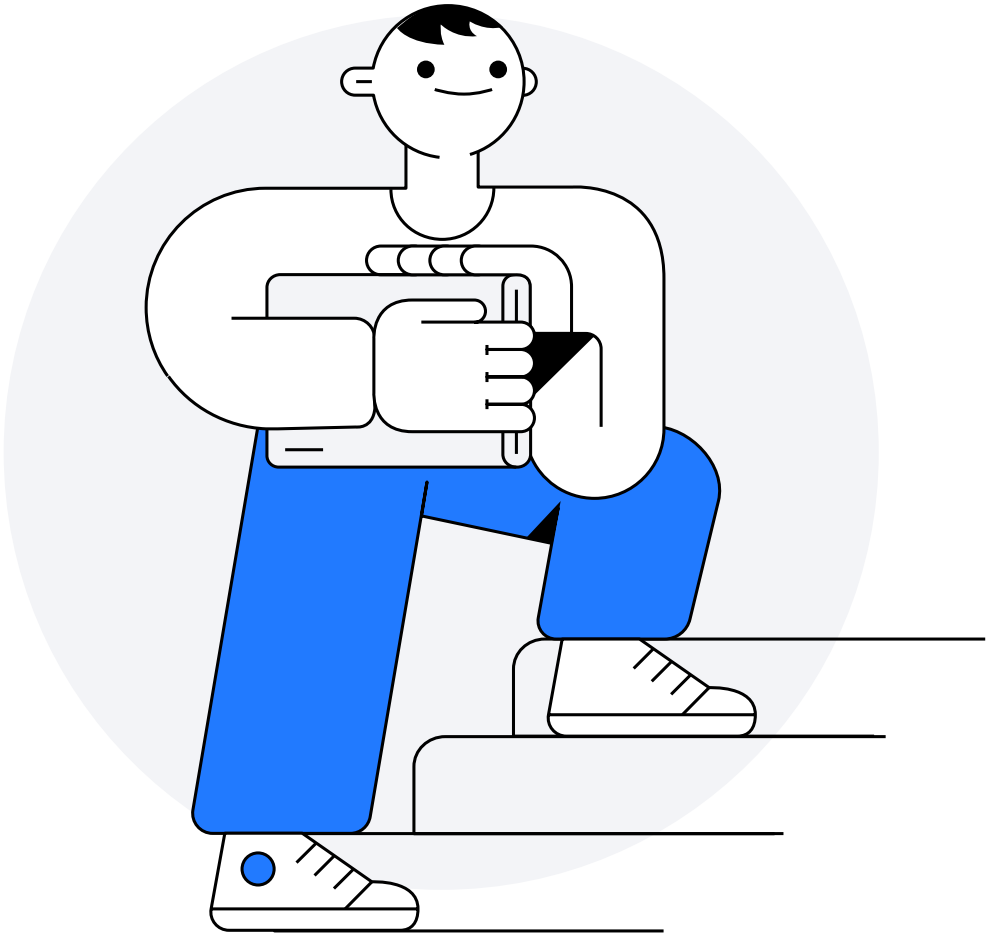
1. Существует несколько классификаций информационных войн и операций
2. Современная информационная война проходит и в технологическом, и в психологическом полях
3. Можно выделить некие общие стратегии ведения информационных войн

Ваши вопросы

Итоги занятия

1. Узнали, что такое угрозы информационной безопасности и каковы их источники
2. Разобрались, что такое информационные войны и какими они бывают
3. Рассмотрели примеры современных информационных войн

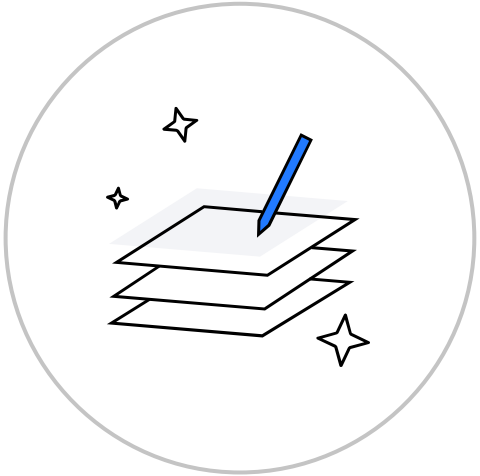
Домашнее задание



Домашнее задание

Цель: проверить знание и понимание пройденного на лекции и вебинаре материала

Формат выполнения: тест из 10 вопросов на платформе



Дополнительные материалы

Аналитические материалы

Тренды и прогнозы в сфере информационной безопасности

Почитать

- Информационные войны. Результаты исследования
- История возникновения информационных войн и их трансформация в современных условиях

Посмотреть

- Русские хакеры. Начало

Ваши вопросы

Угрозы информационной безопасности

Информационные войны

Оксана Докучаева