Кибернетические и информационные войны: основные вызовы и игроки

120 стр. PDF 2022 г.

В пособии введены понятия о кибервойне и информационной войне. Рассказано об искусственном интеллекте и его влиянии на создание кибероружия и преимущество в кибервойнах. В работе уделено внимание почерпнутым из открытых источников OSINT методам разведки в условиях ведения кибервойны или информационной войны. Подробно освещена методика ведения информационной войны в Интернете, описаны как психологические, так и технические методы ее ведения. Описаны доктрины ведения кибервойны для различных государств: Российской Федерации, США, Китая и др.

Введение

Глава 1. Основные понятия и определения

Глава 2. Концептуальные аспекты кибербезопасности

- **2.1. Угрозы и риски кибербезопасности, привнесенные цифровой трансформацией, в условиях кибервойны**
- **2.2. Руководящие указания по планированию кибербезопасности**
- **2.3. Кибербезопасность электронного правительства и персональных данных**
- **2.4. Вопросы защиты персональных данных, находящихся в облаке, от киберугроз**
  - 2.4.1. Основные источники киберугроз для элементов распределенной ИСПДн
  - 2.4.2. Управление рисками транспортной среды корпоративной сети ЭП

Глава 3. Искусственный интеллект и кибербезопасность

- **3.1. Влияние ИИ на кибер- и информационную безопасность**
  - 3.1.1. Барьеры и проблемы, осложняющие использование ИИ в кибер- и информационной безопасности
- **3.2. Нападение и защита: ИИ меняет соотношение сил**
  - 3.2.1. Экономия инвестиций благодаря ИИ
  - 3.2.2. Противостояние машин
  - 3.2.3. Политика в отношении использования ИИ для укрепления национальной безопасности
- **3.3. Некоторые уроки трансформирующей технологии ИИ**

Глава 4. Концептуальные основы проведения кибер- и сетецентрических войн

Глава 5. Разведывательные операции в кибервойнах: разведка в открытых источниках

- **5.1. Базовые принципы OSINT**
- **5.2. Терминология OSINT**
- **5.3. Роль OSINT при проведении объединенных наземных операций**
  - 5.3.1. Функции OSINT при проведении боевых операций
  - 5.3.2. Процесс ведения разведки
  - 5.3.3. Требования к планированию и оценка процесса сбора информации
  - 5.3.4. Планирование и подготовка разведки в открытых источниках
  - 5.3.5. Определение операционной среды
  - 5.3.6. Описание влияния внешних факторов на проведение операции
  - 5.3.7. Оценка угроз
  - 5.3.8. Определение сценариев развития угроз
- **5.4. Подготовка ведения разведки в открытых источниках**
- **5.5. Создание структуры OSINT**
- **5.6. Оперативные и технические базы данных открытых источников**
  - 5.6.1. Факторы, влияющие на процессы планирования и подготовки в OSINT
  - 5.6.2. Надежность открытых источников
  - 5.6.3. Достоверность информации в открытых источниках
  - 5.6.4. Дезинформация
- **5.7. Кибербезопасность и OSINT**
  - 5.7.1. Ситуационная осведомленность о киберпространстве и кибербезопасности
- **5.8. Инструментарий для OSINT**
  - 5.8.1. Лучшие инструменты OSINT

Глава 6. Методы анонимизации и деанонимизации в Интернете при ведении кибер- и информационных войн

- **6.1. Деанонимизация противника в кибероперациях. Основные методики**
- **6.2. Базовые схемы анонимизации в сети Интернет**

Глава 7. Проведение разведывательных и исследовательских операций в даркнете в целях кибер- и информационных войн
7.1. Как получить доступ в даркнет
7.2. Проблемы сбора доказательной базы в даркнете
Глава 8. Информационная война: технологии ведения
8.1. Цели и задачи информационной войны
8.1.1. Методы ведения информационной войны
8.2. Наиболее частые приемы пропаганды и рекламы, используемые в информационной войне
8.3. Принципы построения смысловых конструкций в информационной войне
8.4. Технологические приемы, используемые специалистами информационных операций в Интернете
8.4.1. Особенности проведения информационных операций в Интернете
8.4.2. Факторы анонимности в информационной войне
8.4.3. Системы рейтингов в Интернете
8.5. Методы проактивной защиты в информационных войнах
8.5.1. Ответные шаги на информационную атаку
8.5.2. Стратегия противодействия: поэтапный план
8.6. Технические аспекты информационных операций
8.6.1. Распространение материала в Интернете: основные техники
8.7. Приемы противодействия информационным атакам в Интернете
8.8. Подготовка контента в рамках ведения информационной войны
8.8.1. Прямые способы распространения информации в инфовойнах в сети Интернет
8.8.2. Методика работы с блогами, сайтами, форумами
8.9. Сервисы SMM в информационной войне
8.10. Борьба с фейками в Интернете: фактчекинг
8.10.1. Фактчекинг: базовые принципы
8.10.2. Рекомендации по фактчекингу от World Association of News Publishers
Глава 9. Программы НАТО по информационной и кибербезопасности
9.1. Развитие технологии 5G
9.2. Программа SATCOM (Satellite Communication)
9.3. Программа STRATCOM (Strategic Communications)
9.4. Концепция AICA (Autonomous Intellectual Cybersecurity Agent)
Глава 10. Кибернетическое командование и кибервойска США
Глава 11. Россия. Кибервойска
11.1. Стратегия кибербезопасности РФ
11.2. Система ГосСОПКА
11.2.1. Структура ГосСОПКА
Глава 12. Китай. Кибервойска
12.1. Кибервойну с Америкой ведут китайские хакеры в погонах
Глава 13. Израиль. Силы самообороны ЦАХАЛ. Кибервойска
13.1. Израиль закроется «железным куполом» от кибервойны
13.2. Вирус атакует иранские ядерные обьекты
13.3. Катастрофа на иранском ракетном полигоне 12 ноября 2011 года
Глава 14. Кибервойска Северной Кореи
14.1. Коммерческие атаки КНДР на соседние страны
14.2. Поторопились: преждевременный удар WannaCry
14.3. Вредоносная деятельность группировок Lazarus и APT37
Глава 15. Южная Корея: повышение уровня кибербезопасности
15.1. Институциональные основы обеспечения кибербезопасности Республики Корея
Заключение
Приложение 1. Указ. О дополнительных мерах по обеспечению информационной безопасности РФ
Приложение 2. Информационная безопасность. Документы
Список источников