

# **Лекция 12. Компьютерная разведка**

1. Цель и общая характеристика компьютерной разведки.
2. Классификация компьютерной разведки.
3. Методы добывания информации из автоматизирован-ных систем обработки данных (АСОД) противника.
4. Промышленный шпионаж и конкурентная компьютер-ная разведка.

# **1. Цель и общая характеристика компьютерной разведки (КР)**

**Цель разведок:** добыча конфиденциальной информации.

**Разведка:** агентурная и техническая.

**Техническая разведка:** выделяет некий "материальный носитель" информации и ее "содержание" (смысл, семантика).

**Информация** – это:

- 1) носитель информации, имеет физическую природу (акустическую, э.м, электрическую и т.п. ), могут быть иные формы;
- 2) «содержание» (смысл) информации, появляется в голове.

**Техническая разведка использует “канал”:**

- 1)источник информации (объект защиты);
- 2)среда передачи данных;
- 3)средство добывания информации, инструмент ТР.

**Компьютерная разведка:** получение информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования.

## **2 Классификация КР**

**Компьютерная разведка предполагает:**

- создание ТКУ;
- использование ТКУ.

**Цели создания ТКУ - получение:**

- 1) данных, сведений, обрабатываемых, передаваемых и хранимых в компьютерных системах и сетях;
- 2) характеристик программных, аппаратных и программно-аппаратных комплексов;
- 3) характеристик пользователей компьютерных систем и сетей.

**Технические средства КР:**

- Радиозакладки;
- Вирусы;
- Недекларируемые средства ПО;

**КР использует угрозы, связанные с добыванием информации из:**

- 1) компьютерных систем и сетей;
- 2) характеристик их программно-аппаратных средств;
- 3) пользователей.

**Использует:**

**1. Семантический анализ** и обработка добытой фактографической и ссы-лочкой информации из общедоступных ресурсов или конфиденциальных источников в компьютерных системах и сетях с созданием специальных информационных массивов.

**2. Программно-аппаратные закладки** и НДВ, обеспечивают добывание данных путем использования заранее внедренных изготовителем прог-раммно-аппаратных закладок, ошибок и НДВ компьютерных систем и сетей.

**3. Вирусные угрозы**, обеспечивают добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами.

**4. Разграничительные угрозы**, обеспечивают добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе преодоления средств разграничения доступа (НСД к информации в АС), а также реализация НСД при физическом доступе к компьютеру или компьютерным носителям информации;

**5. Сетевые угрозы**, обеспечивают добывание данных из ЛВС (сетей), путем зондирования сети, инвентаризации и анализа уязвимостей сетевых ресурсов с последующим удаленным доступом либо блокированием доступа к ним, модификация, перехват управления либо маскирование своих действий;

**6. Потоковые угрозы**, обеспечивают добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров;

**7. Аппаратные угрозы**, обеспечивают добывание информации и данных путем обработки сведений о аппаратуре, оборудовании, модулей с после-дующим анализом для выявления их технических характеристик и возможностей, использованием другими типами ТКУ;

**8. Форматные угрозы**, обеспечивают добывание информации и сведений путем "вертикальной" обработки, фильтрации, декодирования и других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем в информацию для последующего ее наилучшего представления пользователям;

**9. Пользовательские угрозы**, обеспечивают добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной

### **3. Методы и средства добывания информации из автоматизированных систем обработки данных противника и возможности защиты от ТКР**

Выделяют ТКР, обеспечивающие добывание информации из:

- 1) компьютерных систем и сетей;
- 2) характеристик их программно-аппаратных средств;
- 3) характеристик пользователей.

РД ФСТЭК России выделяют 6 подсистем защиты в АС: 1) управления доступом;  
2) регистрации и учета;  
3) обеспечения целостности;  
4) криптографической защиты;  
5) антивирусной защиты;  
6) обнаружения вторжений.

## **4. Промышленный шпионаж и конкурентная компьютерная разведка**

**1993 год,** Билл Клинтон распорядился, чтобы шпионаж в интересах американской промышленности стал одной из главных задач ЦРУ.

**Директор ЦРУ** получил право привлекать специалиста из любой госструктуры для решения собственных задач. Возникает и развивается новая парадигма управления — менеджмент, основанный на знаниях.

**Более 80%** оперативной и стратегической информации, необходимой для профессиональной деятельности компании, органа власти, международной организации или иной структуры управления (далее - Корпорация), может быть получено через Интернет.

По последним оценкам, ресурсы Всемирной паутины составляют 550 млрд. документов, из которых 40% доступны бесплатно. Навигацию в этом многообразии обеспечивают более миллиона поисковых систем, каталогов, баз данных.

**Конкурентная разведка:** комплекс мероприятий по информационо-аналитическому обеспечению менеджеров знаниями о состоянии и тенденциях изменения внешнего окружения Корпорации.

В основе конкурентной разведки лежит анализ доступной информации о бизнесе и своевременное представление результатов такого анализа. “В отличие от деловой разведки, конкурентная разведка – это анализ, ориентированный на будущее, он помогает менеджерам принимать наилучшие решения”. Получаемое таким образом информационное преимущество переводится в устойчивое конкурентное превосходство Корпорации

### **Цели создания службы конкурентной разведки:**

- 1) управление рисками бизнеса;
- 2) раннее выявление угроз, уязвимостей, возможностей и иных факторов влияния на успех бизнеса;
- 3) обеспечение конкурентных преимуществ за счет своевременного принятия нестандартных решений.

## **Задачи службы конкурентной разведки:**

- 1) сбор важной для Корпорации информации на регулярной основе;
- 2) автоматический предварительный анализ потока собираемых сведений (классификация);
- 3) своевременное информирование руководителей и персонала Корпорации о критически важных событиях;
- 4) управление отношениями с клиентами;
- 5) обеспечение простого доступа к знаниям Корпорации персонала и клиентов;
- 6) оперативный анализ неструктурированной и структурированной информации (извлечение новых знаний)

## **Сфера интересов конкурентной разведки:**

- 1. Конкуренты.** Наблюдение за конкурентами, кредиторами, заемщиками, контрагентами Корпорации. Выявление структуры предложения, оценка технологического потенциала конкурентов и выявление их ведущих специалистов.
- 2. Политика.** Выявление групп давления и отдельных лоббистов, их использование для продвижения благоприятных для Корпорации политических решений.
- 3. Государство.** Использование органов власти для пресечения противоправной деятельности конкурентов, инициация проверок и судебных расследований.
- 4. Криминал.** Мониторинг правомочности действий интересующих Корпорацию персон и юридических лиц, прогнозирование и профилактика афер в сфере деятельности Корпорации, сбор доказательств для судебного преследования и иного противодействия, управление рисками бизнеса.
- 5. Право.** Мониторинг законодательства в области жизненных интересов Корпорации, профилактика обстоятельств непреодолимой силы
- 6. Потребители и корпоративные клиенты.** Учет и анализ претензий, предпочтений и предложений; персонаификация и улучшение качества обслуживания, назначения и перемещения руководителей, контакты с конкурентами.
- 7. Заказы.** Наблюдение за объявлениями конкурсов, тендеров, подрядных торгов, распределением бюджетных и иных крупных заказов, выявление потенциальных заказчиков и инвесторов, изучение технологических и иных преимуществ победителей конкурсов.
- 8. Маркетинг.** Сбор информации о крупных сделках, изменении цен, спроса и предложения, появлении конкурирующих продуктов и услуг.
- 9. Финансы.** Мониторинг предложений кредитных организаций, грантодателей, благотворительных фондов, спонсоров, властей
- 10. Нематериальные активы.** Выявление и сбор доказательств для судебного преследования субъектов, незаконно использующих объекты интеллектуальной собственности.
- 11. Патенты.** Мониторинг данных для оспаривания мешающих бизнесу охранных документов.

**12. Связи с общественностью.** Социологический мониторинг публикаций и высказываний о деятельности Корпорации, определение реакции на распространяемые Корпорацией материалы, обнародование информации об успехах Корпорации и провалах конкурентов, создание информационных поводов для прессы.

**13. Технологии.** Мониторинг научно-технической информации, технологических новинок и патентов в области интересов Корпорации.

**14. Безопасность.** Контроль утечки конфиденциальной информации и техдокументации Корпорации.

**15. Кадры.** Слежение за действиями нужных или опасных для Корпорации специалистов (руководители и менеджеры конкурирующих организаций, собственный персонал, политики, учёные и иные носители секретов), оценка направлений ротации кадров, изучение мотивов увольнений, выявление потенциальных агентов Корпорации.

**16. Подразделения.** Слежение за работой филиалов, представительств, дочерних фирм

**17. Средства сбора и анализа.** Выявление и испытание средств и методов слежения, обработки и анализа.

**18. Источники информации.** Мониторинг появления и контроль качества ресурсов Интернета - источников нужных для Корпорации сведений

**19. Иные данные.** Сбор материалов по всем иным значимым для Корпорации проблемам (прочие риски профессиональной деятельности и управления), описанным корпоративным классификатором области жизненных интересов

**Spyware** - это программа, которая посыпает информацию с вашего компьютера на какой-либо другой, причем, это происходит без вашего ведома и согласия.

Пересылаемая информация может включать все, что находится на вашем компьютере или доступно с него.

Большая часть **spyware** рассчитана на пересылку демографической информации, например, адресов посещаемых вами страниц в Интернете или адресов электронной почты, обнаруженных на дисках вашего компьютера.

**КОНЕЦ**