ГЛАВА 5

КИБЕРШПИОНАЖ, КИБЕРРАЗВЕДКА И КИБЕРКОНТРРАЗВЕДКА

Рассматриваются проблемы кибершпионажа, киберразведки и киберконтрразведки: классификация, способы, объекты, основные источники угроз, цели, задачи и методы работы «профессионалов». В рамках отдельного параграфа рассмотрены основные особенности применения методов стратегической киберразведки как способа управления корпоративными рисками. На основании представленного материала сформулированы специфические требования к подготовке (обучению) нового поколения специалистов по информационной и кибербезопасности.

Рассмотрена организационная структура, основные функции, цели и задачи главного управления киберконтрразведки США – мирового лидера в этом направлении, представлен краткий анализ типовых ежегодных отчетов главного управления о киберугрозах.

На конкретных примерах здесь также продемонстрирован тот факт, что расследование кибератак сегодня превратилось как в высокоприбыльный бизнес, так и в важный инструмент политической борьбы. Понятно, что решать задачи киберразведки и тем более киберконтрразведки «вручную» уже становится невозможным даже с помощью «талантливых личностей». Поэтому здесь детально рассмотрены как коммерческие (приобретаемые за «большие деньги»), так и некоммерческие (бесплатные – open sourse) автоматизированные программно-аппаратные платформы: в частности – практические особенности автоматизации этих процессов с помощью наиболее популярной Threat Intelligence Platform: основные этапы алгоритма реализации, стандартный цикл процесса контрразведки и др.

5.1. Классификация, способы и объекты кибершпионажа

5.1.1. Классификация кибершпионажа

Кибершпионаж – несанкционированное, незаконное получение доступа к защищенной информации с различными целями. Осуществляемое за счет «обхода» систем компьютерной безопасности. Для этого «кибершпионами» применяются специальные шпионские программы, аппаратные и программные трояны. Взлом систем безопасности осуществляется через Интернет и локальные сети, а также посредством физического доступа. Во многих странах кибершпионаж сегодня расценивается как преступление, но квалификация отдельно взятых деяний «кибершпионов» зависит уже от конкретных обстоятельств дела.

В зависимости от *целей* кибершпионаж может подразделяться на следующие категории:

– *политический* кибершпионаж;
– *экономический* кибершпионаж;
– *военный* кибершпионаж;
– *смешанный* кибершпионаж.

Под экономическим кибершпионажем обычно понимается как *кража* непосредственно финансовой информации, так и *стремление* незаконно проникнуть в базу данных с инновационными разработками в области науки, техники, промышленности, включая ноу-хау.

В качестве еще одного критерия для классификации кибершпионажа используются следующие *уровни*:

– международный;
– государственный;
– региональный.

По мере постоянного увеличения масштабов этого явления в мире растет и степень его опасности. Большинство действующих хакерских групп и группировок обычно не ограничиваются рамками какой-либо одной страны.

Также кибершпионаж классифицируется и по *объекту нападения*. Действия злоумышленников могут быть направлены против:

– высокопоставленных частных лиц,
– предприятий, корпораций, промышленных и энергетических инфраструктур,
– государственных структур, включая оборонные ведомства.

Классификации кибершпионажа различными экспертами осуществляются и на других основаниях: в зависимости от размеров причиненного ущерба, способов воздействия, протяженности во времени, количества вовлеченных лиц, юридических последствий и др.

5.1.2. Способы осуществления кибершпионажа

Способы осуществления кибершпионажа постоянно развиваются сообразно с появлением и вводом в эксплуатацию нового ПО, постоянным увеличением роли инфокоммуникационных технологий в жизни человека и общества. К основным способам кибершпионажа обычно относят:

1. вредоносные и шпионские программы. Потенциально угрожают всем, кто пользуется Интернетом, включая рядовых владельцев страниц в соцсетях;
2. программы-импланты (недекларированные возможности). Преступники используют имеющийся в программах код, позволяющий получать несанкционированный доступ к компьютерной системе;
3. целевые атаки (APT). Комплексы киберпреступных действий, проводимые против определенной компании или организации; отличаются высокой степенью эффективности.

Способы кибершпионажа также подразумевают как виртуальные манипуляции, так и совмещенные с физическими методами. К последним прибегают в тех случаях, когда интересующие преступников сведения хранятся на носителе информации, не подключаемом к Интернету и остальным устройствам локальной сети.

5.1.3. Объекты кибершпионажа

Жертвой кибершпионажа в современном мире рискует оказаться практически каждая заметная на рынке компания или государственная организация, не говоря уже об объектах, относящихся к обеспечению национальной безопасности. Кибершпионажем занимаются спецслужбы или хакерские группировки по их заказу. Подобные акты расцениваются как преступление в государстве-жертве, но обычно не квалифицируются таким образом в стране-агрессоре. Абсолютное большинство операций глубоко засекречены, о конкретных событиях только иногда можно узнать по результатам разоблачений в СМИ.

Кибершпионаж может выполняться «наемниками», но нередко атаки осуществляются и противниками (конкурентами) известных политических фигур, политических партий, государств. Он очень тесно переплетается с такими понятиями, как «кибертерроризм» и «кибервойны». Можно констатировать, что *шпионаж в киберпространстве* стал обязательной частью военных и прочих недружественных действий, которые одни страны в современном мире ведут против других.

В *политическом контексте* «кибершпионов» интересуют данные о государственных чиновниках, засекреченные документы, военные отчеты. Добытые сведения используются в политических целях, для получения экономической выгоды, дискриминации, дестабилизации, подрыва авторитета оппонента или правящей партии.

Под постоянным и все возрастающим риском находятся крупные корпорации. В отличие от предыдущего пункта, здесь деятельность хакеров всегда оценивается как преступление (кража интеллектуальной собственности, причинение имущественного ущерба, нарушение коммерческой тайны). Наибольший интерес для «кибершпионов» представляют всевозможные инновационные разработки, ноу-хау, результаты маркетинговых исследований, внутренняя служебная документация, котировки, ведомости, бухгалтерские и финансовые документы и т.п.

Частные лица тоже находятся в зоне риска. Известно, что спецслужбы ряда стран следят за гражданами, прикрываясь борьбой с терроризмом и преступностью (АНБ собирало данные адресных книг миллионов пользователей). В группу риска попадают политические деятели, крупные бизнесмены, ученые, общественные деятели и журналисты. Определенная опасность существует также для их близкого окружения (родственников, знакомых), которое может попасть в группу негласного наблюдения.

5.1.4. Основные источники угрозы кибершпионажа

Угрозы могут исходить от спецслужб и хакерских группировок. Для криминальных элементов кибершпионаж не является самоцелью, но бывает частью их деятельности. Есть группировки, действующие по идеологическим и (или) материальным причинам.

Кибершпионаж может включать физическое проникновение, но в последние годы до 90% всех осуществляемых сегодня атак приходится на Интернет или локальные сети.

«Слабым местом» правительственных организаций, юридических лиц являются их официальные сайты, корпоративные блоги, веб-страницы сотрудников, личные