УДК 334.021

ПРОМЫШЛЕННЫЙ ШПИОНАЖ В КОММЕРЧЕСКОЙ СФЕРЕ

Загребина А.А.
студент,
Вятский государственный университет,
Киров, Россия
Головкова Е.А.
студент,
Вятский государственный университет,
Киров, Россия

Аннотация

Промышленный шпионаж — это не только незаконная деятельность, но и серьезная угроза конкурентоспособности компании и ее дальнейшего развития. Современный мир, где конкуренция только усиливается, делает эту проблему особенно актуальной. Целью исследования является раскрытие понятия промышленного шпионажа, история его развития, виды, средства, известные случаи и какие последствия влечет за собой данное преступление, чтобы компании имели представление о том, на что нужно обратить внимание во избежание утечки конфиденциальной информации. По результатам исследования выявлено, что промышленный шпионаж в настоящее время приобретает новые формы, негативно влияющие на экономическую деятельность. Также были предложены мероприятия по повышению уровня безопасности от промышленного шпионажа.

Ключевые слова: промышленный шпионаж, информация, данные, документы, взлом, информационная безопасность, интеллектуальная собственность

INDUSTRIAL ESPIONAGE IN THE COMMERCIAL SPHERE

Zagrebina A.A.
student,
Vyatka State University,
Kirov, Russia
Golovkova E.A.
student,
Vyatka State University,
Kirov, Russia

Annotation

Industrial espionage is not only an illegal activity, but also a serious threat to the competitiveness of the company and its further development. The modern world, where competition is only intensifying, makes this problem especially relevant. The purpose of the study is to reveal the concept of industrial espionage, the history of its development, types, means, known cases and what consequences this crime entails, so that companies have an idea of what to pay attention to in order to avoid leakage of confidential information. According to the results of the study, it was revealed that industrial espionage is currently taking on new forms that negatively affect economic activity. Measures were also proposed to increase the level of security against industrial espionage.

Keywords: industrial espionage, information, data, documents, hacking, information security, intellectual property

Введение

Промышленный шпионаж — это процесс получения информации, связанной с бизнесом, технологиями, планами развития и т.д. у конкурентов или

других фирм. Целью является получение выгоды и конкурентного преимущества.

Промышленный шпионаж может включать в себя физическое проникновение на территорию конкурента, взлом информационных систем или привлечение сотрудников компании к работе на свою фирму.

Шпионаж является преступлением и может иметь серьезные последствия, такие как юридические споры, потери конкурентоспособности, моральный ущерб и т.д. Поэтому компании должны принимать меры по защите своей конфиденциальной информации, включая использование средств шифрования, контроль доступа к информации и обучение своих сотрудников правилам информационной безопасности.[3]

Целью исследования является изучение проблемы промышленного шпионажа для коммерческой сферы, его влияние на работу компании.

Основными задачами являются:

1. Определение понятия «промышленный шпионаж», историю возникновения и развития.
2. Исследование методов, техники и средств промышленного шпионажа.
3. Проанализировать известные примеры из практики и последствия данного преступления.
4. Дать рекомендации по повышению уровня безопасности от промышленного шпионажа.

Основная часть

Возникновение промышленного шпионажа связано с развитием промышленности и конкуренции между компаниями. Первые случаи промышленного шпионажа относятся к XVIII веку, когда британская королевская монархия использовала шпионов для получения технологических знаний у французских и голландских компаний. [2]

По мере развития технологий и научно-технического прогресса, промышленный шпионаж стал все более распространенным. Сегодня

промышленный шпионаж включает в себя уклонение интеллектуальной собственности, взлом компьютерных систем и мобильных устройств, кражу конфиденциальных документов, найм шпионов-сотрудников и другие методы.

Главными жертвами промышленного шпионажа являются компании, занимающиеся высокотехнологичными и военно-промышленными проектами. Цели шпионажа могут быть различными, например, получение конкурентной информации, кража технологий или уклонение интеллектуальной собственности.

Борьба с промышленным шпионажем осуществляется через защиту интеллектуальной собственности, укрепление безопасности компьютерных систем, аудит безопасности, установку мониторинговых систем и привлечение правоохранительных органов.

Прогресс техники очень сильно повлиял на развитие промышленного шпионажа в последние годы. Современные технологии позволяют шпионам быстро и легко получать доступ к конфиденциальной информации.

Среди основных технологий, которые используются в промышленном шпионаже, можно выделить следующие:

1. Электронные устройства подслушивания и видеонаблюдения — это камеры и микрофоны, установленные в помещении, различные гаджеты, вроде умных часов и телефонов, которые могут потенциально быть использованы для шпионажа.

2. Компьютерная шпионаж - злоумышленники используют различные программы и вирусы для получения доступа к компьютерам, сетям и данных. Они могут удалять, изменять и копировать конфиденциальную информацию.

3. Социальная инженерия — это методы манипулирования людей, чтобы они делились конфиденциальной информацией. Это может быть выполнено через различные каналы связи, такие как социальные сети, электронная почта, телефонные звонки и т.д.

4. Физический доступ к защищенным помещениям - шпионы могут использовать приемы для получения доступа к помещениям, где хранится конфиденциальная информация. Например, это может быть взлом замков или проникновение через окна или канализационные люки.

5. Организации незаконного доступа - злоумышленники могут использовать сторонних подрядчиков, сотрудников или даже бывших сотрудников, чтобы получить доступ к конфиденциальной информации.

Разработка новых и совершенствование существующих технологий в области промышленного шпионажа создает новые вызовы для компаний, которые должны совершенствовать системы безопасности и защиты конфиденциальной информации. [4]

Другими, не менее важными направлениями получения открытого доступа к конфиденциальной информации являются:

- доклады на конференциях, симпозиумах и т.д.;
- вопросы, осторожно задаваемые специалистами конкурента на этих мероприятиях;
- попытки пригласить на работу специалистов и заполнение ими с этой целью специальных вопросников;
- беседы со служащими конкурирующих фирм (без нарушения закона);
- наем на работу служащего конкурирующей фирмы для получения требуемой информации;
- изучение выставочных образцов;
- притворные переговоры с конкурентом якобы для приобретения лицензии или для совместной деятельности.

Как и любая другая отрасль, промышленный шпионаж использовал различные инструменты и технологии для получения конфиденциальной

информации о других компаниях. Некоторые из наиболее распространенных средств промышленного шпионажа включают:

1. Обман и взлом паролей. Часто шпионы пытаются получить доступ к конфиденциальной информации, используя обманные и ложные техники. Они могут попытаться подставиться за сотрудника или получить доступ к системам компании, используя украденные или угаданные пароли.

2. Распространение вредоносного кода. Хакеры и шпионы могут использовать вредоносные программы, такие как вирусы, троянские программы или черви, для получения доступа к конфиденциальной информации.

3. Подслушивание и наблюдение. Шпионы могут использовать технологии для подслушивания или наблюдения за сотрудниками компании, например, устанавливая скрытые камеры или скрытые микрофоны.

4. Отслеживание данных в Интернете. Шпионы могут использовать программы для мониторинга активности компании в Интернете, например, отслеживая электронную почту или социальные сети.

5. Наем внутренних агентов. Шпионы могут попытаться нанять внутренних агентов в компании, чтобы они стали их информаторами и предоставляли конфиденциальную информацию.

Это только некоторые из множества средств промышленного шпионажа, используемых в настоящее время. Компании должны принимать меры для защиты своей конфиденциальной информации, включая использование современных технологий защиты данных и обучение своих сотрудников тому, как защититься от шпионажа. [5]

Существует множество известных случаев промышленного шпионажа. Вот некоторые примеры:

1. Компания DuPont была обвинена в том, что сотрудник передал секретную информацию о производстве кевлара конкуренту, компании Kolon Industries. Это привело к судебному разбирательству и к тому, что Kolon

Industries была признана виновной в шпионаже и должна была заплатить 920 миллионов долларов компании DuPont.

2. Конкуренты Ford и General Motors обвиняют друг друга в шпионаже уже много лет. В 2010 году компания General Motors была обвинена Федеральным бюро расследований (ФБР) в том, что она шпионила за компанией Ford и пыталась получить доступ к их секретам.

3. В 2017 году компания Waymo (дочерняя компания Google, занимающаяся разработкой автономных автомобилей) подала в суд на Uber за кражу технологий самоуправляемых автомобилей. Убер был обвинен в том, что он украл технологии, разработанные бывшими сотрудниками Waymo.

4. В 2019 году сотрудник Специального управления по связям с общественностью Минобороны России был взят под стражу в США за шпионаж в пользу России. Сотрудник пытался получить конфиденциальную информацию об американских вооруженных силах и планируемых военных операциях.

Это только некоторые случаи промышленного шпионажа. Подобные преступления не только наносят ущерб бизнесу, но и могут оказывать серьезное влияние на национальную безопасность. [4]

Ответственность за промышленный шпионаж лежит на лице, которое совершает такие действия. В различных странах существуют законы, которые вводят уголовную, административную и гражданскую ответственность за промышленный шпионаж. Наказания за такие преступления могут включать штрафы, тюремное заключение, а также убытки, которые наносит шпионаж вымогателя. Кроме того, компании часто могут использовать юридические средства для защиты своих коммерческих секретов и права интеллектуальной собственности. [1]

Заключение

По результатам исследования выявлено, что промышленный шпионаж является довольно актуальной проблемой в современном мире.

Для повышения уровня безопасности от промышленного шпионажа можно рекомендовать следующие меры:

1. Обучение сотрудников. Проведение регулярных тренингов и семинаров по безопасности информации для сотрудников, в том числе таких, как работа с электронной почтой и социальными сетями, связанные с обработкой и передачей конфиденциальной информации.

2. Управление доступом. Рациональное управление доступом к информации и программному обеспечению, а также к заправочным процессам, построенным на привилегиях, может помочь предотвратить неправомерный доступ к конфиденциальной информации.

3. Шифрование данных. Для хранения и передачи конфиденциальной информации необходимо применять криптографические методы и средства шифрования. Они помогают убедиться в сохранности данных в том случае, если они попадут в руки злоумышленников.

4. Физическая защита. Применение мер физической защиты, таких как использование замков, контроля доступа, видеонаблюдения и т.д., может помочь предотвратить физический доступ к конфиденциальной информации.

5. Защита программного обеспечения. Использование программного обеспечения для защиты компьютеров и сетей от вирусов, взломов и других угроз.

Определение стратегии для охраны конфиденциальной информации может помочь предупредить атаки со стороны злоумышленников и защитить данные и определить стратегию действий при нарушениях. Важно не забывать, что безопасность - процесс постоянный и требует постоянного следования новым тенденциям и угрозам.

Библиографический список:

1. Галактионова Н. В. АКТУАЛЬНЫЕ ВОПРОСЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ // Вестник Хабаровского

государственного университета экономики и права. 2021. №2 (106). URL: https://cyberleninka.ru/article/n/aktualnye-voprosy-ekonomicheskoy-bezopasnosti

2. Пресняков В.А., Дорофеев О.В. КОНКУРЕНТНАЯ РАЗВЕДКА: ПОНЯТИЕ, СУЩНОСТЬ, СООТНОШЕНИЕ СО СМЕЖНЫМИ ПОНЯТИЯМИ // Инновации и инвестиции. 2023. №3. URL: https://cyberleninka.ru/article/n/konkurentnaya-razvedka-ponyatie-suschnost-sootnoshenie-so-smezhnymi-ponyatiyami
3. Недобросовестная конкуренция: учебно- практическое пособие / О. А. Городов, А. В. Петров, Н. А. Шмигельская ; под ред. О. А. Городова. — М., 2020.
4. Пресняков В.А., Дорофеев О.В. КОНКУРЕНТНАЯ РАЗВЕДКА: ПОНЯТИЕ, СУЩНОСТЬ, СООТНОШЕНИЕ СО СМЕЖНЫМИ ПОНЯТИЯМИ. – Текст: электронный - URL: https://cyberleninka.ru/article/n/konkurentnaya-razvedka-ponyatie-suschnost-sootnoshenie-so-smezhnymi-ponyatiyami
5. Шатохина Н.М., Соболева И.С. Современные технологии и методы отбора и набора персонала // Современная наука: Актуальные вопросы, достижения и инновации: сб.ст. конф. / Наука и просвещение - Пенза, 2020. - С. 146-150.

Оригинальность 83%