Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 8, Is. 2, pp. 62-69, 2016

DOI: 10.13187/vesp.2016.8.62
www.ejournal21.com

UDC 34

Use of Methods of Professional Mentalist for the Purpose of Theft of Information

[1] Bogdan T. Kudyma
[2] Artem A. Gonchar

[1] Admiral Makarov State University of Maritime and Inland Shipping, Russian Federation
Dvinskaya Str., 5/7, Saint Petersburg 198035
E-mail: boserov@bk.ru
[2] St. Petersburg University of the Russian Interior Ministry, Russian Federation
Flyer Pilyutova Str., 1, St. Petersburg 198206
PhD (Military Science), Major of the police
E-mail: gonchar.tema@yandex.ru

Abstract

Industrial espionage has the big range of use and a bigger range of implementers. Now, the sufficient attention is paid to technical channels of information leakage though the personnel of the enterprise still are the main source of danger. Worldwide swindlers use skills of professional illusionists for the purpose of deception, and also theft of personal and business information. Unfortunately, this subject is very poorly lit though it is rather actual now as the ordinary inhabitant can easily get on the swindler's tricks. Basic concepts about industrial espionage, with profound consideration of personnel are given in this article as information leakage source, and also definition of the main the technique of mentalist are described and given, in particular research of such equipment as "Cold reading" is given is detailed.

Keywords: cold reading; Fraud; theft of information; leakage channels.

Введение

Промышленный шпионаж появился вместе с промышленностью и является важной частью нашей жизни, в которой существуют различные формы собственности. Суть промышленного шпионажа – это желание приобрести тайны конкурентов для повышения коммерческой выгоды. Целью данного вида шпионажа является нахождение новой информации о коммерческих планах, новейших технологиях, и т.д. Способы получения информации могут быть совершенно разными, от использования высокотехнологических средств до шантажа и подкупа сотрудников конкурирующей компании.

Промышленный шпионаж в основном не несет вреда непосредственно государству, но он все равно является незаконным видом деятельности, так как нацелен на нарушение конституционных прав граждан. На протяжении всего существования человечества люди ведут различные войны, в современном мире битва идет в основном за информацию и человек использует многовековой опыт военного дела с целью хищения ценных данных у конкурирующей стороны. В данной статье освещены некоторые каналы утечки информации, которые на данное время слабо изучены. Также раскрыты некоторые способы

несанкционированного доступа к мобильным телефонам жертв. И хотя пока зафиксировано очень мало случаев использования этих приемов с целью ведения промышленного шпионажа, но для добывания персональных данных они проявляются постоянно. Много где приведены примеры шарлатанства знахарей и астрологов, но этот материал не обобщен и не установлена потенциальная опасность осуществления этой угрозы. Следует также заметить, что по данной тематике очень мало информации по сравнению с анализом других каналов утечки.

Материалы и методы

Основным источником для написания данной статьи стали официальные документы, регламентирующие действия правоохранительных органов по обеспечению информационной безопасности, а также последние сведения о методиках, которыми пользуются профессиональные иллюзионисты узкой направленности, а именно – менталисты.

Методологическую основу данного исследования составили логические приемы, определения, описания, анализа и синтеза. Также использован общенаучный метод анализа.

Обсуждение

Рассмотрим основные способы разведывательных действий. В основном, все методы хищения информации, в независимости от того, против кого они принимаются, можно распределить по трем основным категориям:

• на основе открытых источников;
• путем использования субъектов – носителей информации;
• через технические каналы.

К первой категории относятся методы добывания информации, основанные на анализе большого количества общедоступных источников. К таким можно отнести книги, газеты, технические и научные выставки, официальные сводки данных и отчеты, а также отдельное внимание стоит уделить рекламным материалам. Данным методом пользуется большинство разведок мира.

Чем больше материалов дает в общее пользование оппонент, тем больше требуется персонала для этой работы, также стоит упомянуть, что коллектив должен состоять из высоко квалифицированных аналитиков, которые могут анализировать большой объем информации, отсеивать ненужные данные и определять важную информацию. Главными направлениями получения открытого доступа к конфиденциальной информации здесь являются:

1. Доклады на конференциях, симпозиумах и других собраниях;
2. Вопросы, осторожно задаваемые специалистами;
3. Попытки пригласить на работу сотрудников конкурирующей фирмы и заполнение ими при этом специальных вопросников;
4. Прием на работу, обычно с резким увеличением оклада служащего конкурирующей фирмы (своего рода законный подкуп);
5. Изучение выставочных образцов;
6. Притворные переговоры с конкурентами о приобретении лицензии или совместной деятельности и другие.

Большинство этих методик уже давно используются заграницей.

Главной особенностью информации является ее свойство постоянно накапливаться, и даже если вы дали какую-либо малозначимую информацию, она может в связи с уже имеющейся или с поступившей в дальнейшем стать очень ценной для конкурентов. Это может быть обычная реклама или неподготовленное интервью. Всегда стоит анализировать исходящий поток информации для понимания, возможных представлений оппонента о вас, либо о вашей компании. Интересной особенностью данного канала утечки является то, что противоборствующая компания может выдавать видоизмененную, либо полностью ложную информацию. Таким образом, через открытые источники можно дезинформировать конкурента [1, 2].

Использование субъектов в качестве хранителей информации относится к другой группе методов промышленного шпионажа. Основная разница в том, что из всех возможных

видов источников информации люди не только могут хранить информацию, но и иметь намерения нанесения вреда предприятию в которой они числятся. В отличие от технических устройств, по отношению к людям можно использовать такие методы как: шантаж, подкуп или стандартный обман, при этом люди не только переносят и распространяют информацию. Их функционал гораздо больше, есть множество способов, с помощью которых они могут навредить промышленному производству. При определенных обстоятельствах люди способны скрывать, воровать, продавать информацию и совершать иные криминальные действия вплоть до вступления в устойчивые преступные связи со злоумышленниками. Правда, процесс принятия кандидата в агенты является достаточно сложным. Вначале проводится оценка и разработка кандидата, то есть изучение его личных качеств и способностей, а также изыскание способов его наиболее эффективной вербовки и использования [1].

Далее производится сама вербовка путём шантажа, подкупа, идейных соображений, личного неприятия руководителя компании и т. д. В большинстве случаев завербованному агенту не дают достоверную информацию об истинном работодателе. В дальнейшем при создании дополнительных рычагов контроля, в основном финансовых (но возможны и другие), агенту раскрывают истинное имя работодателя. Интересно то, что путем поощрений и одобрений можно добиться от агента гораздо большего, нежели при применении угроз и подобных средств. Поэтому умные вербовщики пытаются создать дружеские отношения с завербованным агентом. Выявление скрытого агента – весьма нелегкая задача, требующая определенных навыков оперативной работы. Нужно стремиться организовать деятельность фирмы так, чтобы большинство персонала не обладало полной информацией. Это лучший способ обезопасить этот канал утечки [2].

Третий канал утечки информации – технический. По большей части это использование подслушивающих устройств. Для затруднения утечки информации по этим путям необходимо использовать специально оборудованные помещения для ведения деловых бесед. Организовать максимально жесткий учет и строго регламентировать порядок работы с деловыми документами. Узаконить круг лиц, допускаемых к тем или иным внутрифирменным секретам, запретить сотрудникам вести служебные переговоры с домашних телефонов. При посторонних нельзя называть конфиденциальную информацию, такую как имя, фамилию и отчество собеседника [1].

Многие из нас хоть раз сталкивались с людьми, которые пользовались услугами экстрасенсов либо других людей подобного рода деятельности. Люди этой профессии очень быстро входят в доверие к своим клиентам, они как личный психолог, которому клиенты доверяют свои тайны, в свою очередь очень подверженные влиянию экстрасенсов. В этом и состоит главная опасность технологии менталистов. Таким же образом ценная информация от ваших сотрудников может уйти к конкурирующим фирмам. Методики фокусников можно использовать для создания рычагов давления на людей. Если злоумышленник вошел в доверие к одному из ваших подопечных, он может внушить ему, что в вашей компании злая аура, или его предки хотели бы зла вашей деятельности. Простор использования техник профессиональных менталистов огромен и разнообразен [3].

Для начала ответим на вопрос: – «Что же такое ментализм?». Это мастерство психологических опытов (англ. Mentalism) — вид исполнительского искусства, демонстрация на публике психологических экспериментов, опытов и «экстрасенсорных» способностей, таких как: телепатия, ясновидение, психокинез и др., а также выдающихся способностей памяти и быстрых вычислений. Фокуснику, занимающемуся этим видом деятельности порой надо выведать личную информацию у жертвы, либо тайно получить информацию от своего компаньона, а также проделывать другие манипуляции, связанные с информацией или хранителями.

Ментализм имеет длинную историю. Маги, чародеи и волшебники, пророки и оракулы известны со времён античности, сведения о них содержатся в дошедших до нас древнегреческих и древнеримских текстах, в Ветхом Завете и многих других исторических источниках. Как вид искусства, ментализм получил развитие в XIX веке в связи с развитием в обществе интереса к спиритизму и медиумизму. Ментализм использует принципы и навыки, схожие с другими видами иллюзионизма. Некоторые из исполнителей (мистификаторы) заявляют, что в действительности обладают экстрасенсорными

способностями (Вольф Мессинг, Ури Геллер), другие утверждают, что в их выступлениях нет ничего сверхъестественного (Деррен Браун, Юрий Горный) и в их номерах используются достижения науки и знание человеческой психики и физиологии [3, 4].

Некоторые менталисты отделяют своё искусство от других видов сценической магии, однако во многих выступлениях сочетаются элементы как психологических опытов, так и иллюзий.

В своей работе я хочу разобрать только одну, но очень весомую методику – "холодное чтение". Для ознакомления приведу краткий список методик и их описание, которыми пользуются профессиональные менталисты при работе на публике.

1) Холодное чтение

Человек, практикующий холодное чтение, может получить большое количество информации о субъекте, не имея до этого момента никакой информации о нем. Это делается при помощи анализа языка тела, возраста, стиля одежды, прически, пола, сексуальной ориентации, религии, расы или этнической принадлежности, уровня образования, манеры речи, места происхождения и т.д. Практикующие холодное чтение обычно используют догадки, которые имеют статистически высокую вероятность оказаться верными, быстро корректируя свои предположения в зависимости от реакции субъекта, на котором используется эта техника. Если догадка оказалась неудачной, то внимание переносится на другую тему, тогда как на верной догадке внимание заостряется [5].

2) Сценическое воровство.

Сценическое воровство отличается о обычного карманичества тем, что внимание жертвы приковывают к другим объектам. Создается много каналов связи с подопечным, через постоянные касания, обсуждение, указывание на какой-либо объект с целью отвлечения внимания. Также задаются вопросы, чтобы заставить жертву задуматься о чем-то и уйти в себя. Такое переполнение информацией скрывает истинные действия манипулятора. Обычно происходит при демонстрации другого трюка/фокуса, но может быть применено и при других обстоятельствах. Может быть использовано не только с целью кражи предмета, но и для подбрасывания чего-либо в карманы жертвы [6].

3) Использование скрытых приспособлений – гиммиков.

Гиммики – это приспособления, которые зрители обычно не видят, а если и видят, то не догадываются об истинном предназначении объекта. Это могут быть такие приспособления как:

a) Утяжки. Служат для быстрого перемещения объектов из рук в карманы/рукава исполнителя, могут быть использованы с целью кражи небольших технических устройств и других носителей информации.

b) Свамми. Гиммик, представляющий собой пишущие устройство, которое крепится на палец/ часть пальца, допустим на ноготь.

c) Технические устройства для передачи информации. Фокусники для получения и передачи информации могут использовать такие каналы связи как: световую, вибрации, магнитные поля, микронаушники, шифровку информации при диалоге и другие.

Большинство людей не верят в экстрасенсов, но значит ли это, что они защищены? Разве это гарантирует им защиту от провокации со стороны менталиста? К сожалению, нет! Большинство людей не верят в сверхспособности, так как не сталкивались с ними в реальной жизни. Но опытный фокусник создаст отличную иллюзию, которая пошатнет образ мышления многих [6].

Создание авторитета. Одно из главных оружий в арсенале аферистов и мошенников, а также фокусников – это создание образа. Образ строится в основном из одежды, манеры речи и поведения. Но более сильное впечатление оказывает наглядный эффект. Если вам порекомендует вещь ваш знакомый, то вы будете отдавать ей предпочтение при выборе из многих. Но Аферист, да и фокусник редко имеет доступ к вашим родственникам и друзьям (хотя имеет доступ ко всей информации о вас в интернете), поэтому он может подстроить ситуацию, когда вы будете очевидцем демонстрации его способностей. Люди, которые используются в этом спектакле, могут быть подставными, либо может использоваться сарафанное радио. Примеров таких приемов множество. Допустим, вы становитесь свидетелем сделки года, при вас проходит одна или несколько сделок и каждый покупатель обогащается, все это создает отличный образ продавца. Таким нехитрым методом сейчас

ведется интернет-мошенничество на многих торговых площадках в интернете, когда пользователь может создать много личностей продавцов и еще больше покупателей для накрутки рейтинга первых. Фокусники же используют этот метод для привлечения большей аудитории и усиления эффекта [5].

Представьте, что вы вышли из офиса и видите толпу людей которые аплодируют, вы заинтересовались происходящим и подошли к толпе, и вот вас вызывает человек, вызвавший эту реакцию. Вы будете считать, что вас вызвал артист, ориентируясь на мнение большинства, так что весь обман уже был совершен. Вас заманили и обманули вашу бдительность, в дальнейшем вас могут обокрасть, либо войти в доверие и воспользоваться сложившейся ситуацией в дальнейшем с целью нанесения вреда вам или организации в которой вы работаете. Фокусники дают иллюзию чуда, но все понимают, что это всего лишь иллюзия. Это все равно, что смотреть на актера, играющего роль, только иллюзионист – это артист, играющий роль волшебника. Так же и злоумышленники отыгрывают нужную им пьесу [6].

Второй основной пункт – это игра на ваших желаниях. Все люди чего-то хотят, манипуляторы пользуются этими желаниями для достижения своих целей. Но они дают лишь иллюзию чего-либо. Поскольку у нас есть какие-то желания, преступник может предложить нам их реализовать. Основные желания, на которых могут сыграть при использовании методик менталистов, это желание узнать будущее, общение с умершими родственниками, желание увидеть чудо, или стремление получить помощь в решении каких-либо проблем, где нужен “духовный наставник”. Когда менталист начинает рассказывать вам о вашем характере или о событиях, произошедших с вами в прошлом, он располагает вашим доверием и дальнейшее общение может быть очень схоже с психологической помощью, что также вызывает желание продолжать общение с исполнителем. Рассмотрим ситуацию: часто есть секретный вопрос для восстановления каких-либо личных данных. Обычно можно задать свой секретный вопрос или воспользоваться шаблонным. Аферист, использовав метод холодного чтения, может втереться в доверие и разузнать что-то о прошлом, кличку животного, либо ваши интересы [4].

Не последнюю роль играет отвлечение внимания. Если вдумываться в происходящее, то рано или поздно можно понять, почему незнакомый вам человек так много знает. И это не ваша аура или линии на руке ему подсказали. Чтобы этого не происходило, манипулятор постоянно нагружает вас информацией. Он без перерыва говорит, отвлекая ваш разум. Перегрузка информацией намного продуктивнее утаиванья информации. При отсутствии фактов вы вынуждены искать их, а при избытке вам приходится сразу фильтровать всю информацию. Может произойти так, что все ниточки будут ложными, и вы вернетесь к отсутствию фактов. Представьте ситуацию, когда вас спрашивают про какой-то объект, в итоге вы заняты рассматриванием объекта и поиска ответа на вопрос, в это же время вас похлопывают по плечу и задают сразу другой вопрос. В этот момент ваша голова занята обработкой слишком большого объема информации, ваше зрение занято, тактильные ощущение сконцентрированы на плече и вы слушаете оппонента, в это время вас спокойно могут обворовывать. Это схоже с методами карманников, когда они воруют при столкновении или в толпе, но тут воздействуют не только на ваши тактильные ощущения, под ударом находится большинство ваших чувств [5].

Результаты

«Холодное чтение» выходит за пределы обычных инструментов манипуляции, таких как внушение и лесть. Подразумевается, что человек, использующий эту методику, должен по мелким деталям, такие как: аксессуары, стиль одежды, цвет кожи, предпочтение в музыке и т.д. составлять характеристику персоны. Причем делается это в реальном времени с использованием только той информации, которая доступна сразу, т.е. вы увидели человека и сразу начинаете анализировать его жесты, вещи и повадки.

Важными чертами также могут быть: акцент, шрамы, общее эмоциональное состояние. Но сделать это все довольно сложно, поэтому в дополнение к этому всегда используются ухищрения. “Чтец” должен использовать размытые фразы, которые можно трактовать неоднозначно, чтобы большинство людей смогли спроецировать это на себя. Также можно использовать фразы наподобие этой: “Временами вы очень уставши и ленивы, но когда вам

нужно закончить проект, вы длительное время можете работать не покладая рук". В этой фразе нет точного указания времени, каждый трактует "длительное время" по-разному, для кого-то это несколько часов, а для других это может быть несколько дней. Тут есть обе крайности для состояния работоспособности, поэтому также подойдет для большинства людей [4, 6, 7].

Очень важно задавать наводящие вопросы, чтобы получать информацию о человеке во время холодного чтения, например, вы можете сказать, что ощущаете его любовь к животным и поинтересоваться есть ли у него домашний питомец. В итоге вы можете перефразировать полученную информацию и выдать ее как свою. Вот пример использования этой техники: "Я чувствую, у вас недавно случилась утрата дорого вам человека". Разберем эту фразу. Во-первых, недавнюю утрату можно трактовать по-разному, вплоть до нескольких лет. Во-вторых, утрата дорогого человека может быть, как смерть родственника, так и расставание с любимым человеком, если человек все же не может вспомнить таких случаев, то можно по-разному трактовать "дорогой": намекните, что это мог быть прибыльный клиент для бизнеса, или даже поломка любимого гаджета. Если человек не может подобрать ни один случай к вашей трактовке, то скорее всего он вам не совсем доверяет и требуется несколько общих фраз, чтобы восстановить авторитет в его глазах. На самом деле, все очень сильно зависит от отношения человека к вам и того, как он идет на контакт. Когда несколько фраз уже зашли на ура, то в дальнейшем вытягивать информацию намного проще [7, 8].

Особое внимание стоит уделить подаче "холодного чтения": для большинства скептиков лучше всего использовать формулировку, что вы анализируете и используете свой богатый опыт в психологии. Но также можно представить это как хиромантию либо астрологию, гадание на картах, чтение ауры. Очень важно найти именно подходящую подачу, либо использовать ту, в которой вы наиболее осведомлены и можете использовать различные термины, которые представят вас как эксперта в этой области. Вся информация, которую вы изливаете на собеседника, обычно более чем на 80% не несет никакого смысла, либо ее можно отнести к большинству людей, либо это просто другая трактовка. Таким образом, хороший манипулятор может понять незнакомца, и у того будет странное чувство, будто манипулятор обладает небольшим количеством специальной власти. Например, Бертам Форер никогда не встречал вас, читателя, все же он предлагает следующее описание вас:

«Вы испытываете потребность в том, чтобы другие люди хорошо относились к Вам и восхищались Вами, и все же Вы склонны быть критическим к самому себе. Хотя Вы имеете некоторые личностные слабости, Вы в целом способны их компенсировать. У Вас есть значительные неиспользованные способности, которые Вы не обратили на свое благо. Внешне дисциплинированный и самоконтролируемый, внутри Вы склонны к беспокойству и неуверенности. Время от времени Вы испытываете серьезные сомнения относительно того, приняли ли Вы правильное решение и сделали ли что-то правильно. Вы предпочитаете известный уровень изменения и разнообразия и становитесь недовольным, будучи притесненным разного рода ограничениями. Вы также гордитесь собой как мыслящим независимо (самостоятельно) и не соглашаетесь с утверждениями других людей без удовлетворительного обоснования. Но Вы сочли неблагоразумным быть слишком откровенным в раскрытии себя другим. Время от времени Вы экстравертированы, приветливы, и общительны, в то время как в другие моменты Вы сосредоточены на самом себе (интровертированы), насторожены и замкнуты. В некоторые из Ваших стремлений (сильных желаний) проявляется изрядная доля нереалистичности.»

Вот — другое описание:

«Близкие люди обманывают Вас, а Ваша честность стоит на пути. Многие возможности, которые были у вас в прошлом, должны были быть осуществлены, но Вы отказались идти на обман других. Вы любите читать книги и статьи, чтобы улучшить свои способности. Фактически, если Вы — всё ещё не имеете личного бизнеса в сфере обслуживания, то Вы должны быть в нём. Вы способны понять народные проблемы, и Вы можете сочувствовать им. И Вы устойчивы, когда сталкиваетесь с упрямством или прямой глупостью. Правоприменительная деятельность была бы другой областью, которую Вы понимаете. Ваше требование правосудия очень сильно» [7].

Последнее описание (характеристика) было от астролога Омара Сиднея. Он даже не встречал Вас, и все же он знает так много о вас. Первый был взят Форером из астрологической книги в газетном киоске.

Также Фокусниками часто используется методика, при которой его партнер ненароком узнает информацию о жертве и передает ее Менталисту, который в дальнейшем выдает эти знания в другой форме. В пример можно привести опыт экстрасенсов, которые собирают крупные залы для спиритических сеансов, где перед началом мероприятия к людям подходят помощники, переодетые в журналистов, либо других посетителей и узнают, зачем жертва пришла на этот сеанс, с кем бы она хотела поговорить из тех кто умер, тем самым давая очень важную информацию для менталиста. Таким образом использование простого алгоритма, при котором жертва рассказывает часть личной информации одному аферисту, помогает другому сблизится с жертвой [9].

Выводы

«Холодное чтение» обычно осуществляется по следующему алгоритму:

- Анализируют человека и пытаются сделать несколько умозаключений о его недавней деятельности, характере или увлечениях, подбираем наилучший способ преподнесения информации (допустим чтение по ауре).

- Дальше происходит сам процесс “чтения”. Первые фразы должны заинтересовать жертву, это может быть рассказ о предчувствии какой-либо опасности для человека, либо ощущения “родственной” связи. Для подкрепления интереса посылается несколько общих фраз, которые подойдут каждому, для создания доверия к вам.

- Затем либо используются полученные ранее выводы, либо задают несколько наводящих вопросов. После одного-двух точных попаданий вы уже можете не боятся ошибиться, поскольку жертва сама будет искать, как ваши слова можно отнести к себе, главное не давать достаточно точных данных, которые могут сильно разнится с истиной.

- Результатом ваших действий будет доверие к вам, а это именно то, что нужно злоумышленникам.

Очень важно знать о методиках “Холодного чтения”. Осознание использования против вас вышеописанных приемов, является основным средством защиты. Когда вы встречаете человека, который видит вас насквозь, не стоит принимать это за истину. Задавайте наводящие вопросы, не позволяйте получить от вас информацию, которую в дальнейшем могут применять против вас. Попробуйте дезинформировать оппонента, если в дальнейшем он будет перефразировать эту информацию и пытаться выдать ее как собственные выводы, вы легко сможете это заметить. Ставьте под сомнения все фразы манипулятора и пытайтесь их проектировать на человека совсем не похожего на вас, если к нему они тоже подходят, значит, против вас используют общие фразы. Самым верным будет прекратить общение и отвергать все предположения манипулятора, тем самым он будет сбит с толку. Призываю вас к бдительности и аккуратности.

Примечания:

1. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. Санкт-Петербург, 2000.
2. Вихров Н.М., Ныркова А.П., Каторин Ю.Ф., Шнуренко А.А., Башмаков А.В., Соколов С.С., Нурдинов Р.А. Анализ информационных рисков. // Морской вестник. № 3(5) 2015. 81-85 с. Издательство "МорВест" (Санкт-Петербург).
3. Браун Д. Уловки разума. Transworld Publishers Limited, 2007.
4. Руденко Б. Феномен Юрия Горного. // Наука и жизнь. 2004. № 1, 2, 3, 4.
5. Роуленд Ян. Книга всеобъемлющих фактов о холодном чтении: Полное руководство по самой убедительной психологической техники манипуляции в мире, 2002.
6. Данилов А.А. Маги криминала. Санкт-Петербург, 2004.
7. Клинт Марш. Менталист. Книга-практикум: как научиться читать мысли и другие практики. Эксмо, 2013
8. Гавенер Торстен. Чтение мыслей: примеры и упражнения. Эксмо, 2013.
9. Домон Джон Б. Секреты менталиста: как понять и противостоять техникам обмана и манипуляций. Эксмо, 2012.

References:

1. Katorin Yu.F., Kurenkov E.V., Lysov A.V., Ostapenko A.N. Large encyclopedia of industrial espionage. Saint Petersburg, 2000.
2. Vikhrov N.M., Nyrkov A.P., Katorin YU.F., Shnurenko A.A., Bashmakov A.V., Sokolov S.S., Nurdinov R.A. Analysis of information risks. // Morskoi vestnik. № 3(5), 2015. pp. 81-85. Publishing house "MorVest" (Saint Petersburg).
3. Brown D. Tricks of the Mind. Transworld Publishers Limited, 2007.
4. Rudenko B. The Phenomenon Of Yuri Gornogo // Science and life. 2004. № 1, 2, 3, 4.
5. Rowland Ian. The Full Facts Book of Cold Reading: A Comprehensive Guide to the Most Persuasive Psychological Manipulation Technique in the World. 2002.
6. Danilov A.A. Magicians of crime. St. Petersburg, 2004.
7. Clint Marsh. Mentalist. Book practical work: how to learn to read mind and other practicing. Eksmo, 2013.
8. Gawener Torsten. Thought-reading: examples and exercises. Eksmo, 2013.
9. Domon John B. Secrets of a mentalist: how to understand and resist to technicians of deception and manipulations. Eksmo. 2012.

УДК 34

Использование методов профессиональных менталистов с целью кражи информации

[1] Богдан Тарасович Кудыма
[2] Артем Александрович Гончар

[1] Государственный университет морского и речного флота имени адмирала С.О. Макарова, Российская Федерация
198035 Санкт-Петербург, ул. Двинская, 5/7
E-mail: boserov@bk.ru
[2] Санкт-Петербургский Университет МВД России, Российская Федерация
198206 Санкт-Петербург, ул. Летчика Пилютова, д. 1
Кандидат военных наук, майор полиции, старший преподаватель
E-mail: gonchar.tema@yandex.ru

Аннотация. Промышленный шпионаж имеет большой диапазон сфер использования и еще больший диапазон средств реализации. В настоящее время, достаточное внимание уделено техническим каналам утечки информации, хотя основным источником опасности по-прежнему является персонал предприятия. По всему миру Мошенники используют навыки профессиональных иллюзионистов с целью обмана, а также кражи личной и деловой информации. К сожалению, эта тематика очень слабо освещена, хотя является достаточно актуальной в настоящее время, поскольку обычный обыватель может легко попасться на уловки мошенника. В данной статье приведены базовые понятия о промышленном шпионаже, с углубленным рассмотрением персонала, как источника утечки информации, а также описывается и дается определение основных техник менталистов, в частности приведено подробное исследование такой техники, как "Холодное чтение".

Ключевые слова: холодное чтение, мошенничество, кража информации, каналы утечки.