Александр Николаевич Обухов
Национальный исследовательский ядерный университет «МИФИ»,
115409, Москва, Каширское шоссе, 31, Россия
e-mail: anobukhov@mephi.ru, ORCID 0000-0002-7241-7177

О ПРИМЕНЕНИИ ПОЛИГРАФА В ИНТЕРЕСАХ ВЫЯВЛЕНИЯ ИНСАЙДЕРСКИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2017.3.07

Аннотация. Данная статья посвящена обоснованию целесообразности проведения проверок с применением полиграфа в интересах выявления инсайдерских угроз информационной безопасности со стороны кандидатов на работу и работающего персонала организации. На основе положений Конституции РФ и Трудового кодекса РФ обоснована законность применения полиграфа в организациях Российской Федерации. На основе положений теории о реакции замирания/бегства/борьбы, а также теории информационного синтеза А.М. Иваницкого обоснована научность психофизиологического метода выявления лжи. На основе статистических исследований, проведённых американскими учёными-полиграфологами, обоснована достоверность получаемой информации. В статье показана возможность и целесообразность проведения в организациях Российской Федерации на законных основаниях проверок с применением полиграфа в отношении кандидатов на работу и работающего персонала с целью выявления инсайдерских угроз и расследования инцидентов, обоснованы их научность и высокая достоверность результатов.

Ключевые слова: инсайдерская угроза информационной безопасности, полиграф, проверка с применением полиграфа, законность проверки, научность метода, достоверность информации.

Для цитирования. **ОБУХОВ, Александр Николаевич.** О ПРИМЕНЕНИИ ПОЛИГРАФА В ИНТЕРЕСАХ ВЫЯВЛЕНИЯ ИНСАЙДЕРСКИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 60-66, july 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/265>. Дата доступа: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.07.

Alexandr Nikolaevich Obukhov
National Research Nuclear University "MEPhI",
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: anobukhov@mephi.ru, ORCID 0000-0002-7241-7177

On the use of polygraph in the interests of identifying insider threats to information security

DOI: http://dx.doi.org/10.26583/bit.2017.3.07

Abstract. The use of the polygraph for detecting potential threats to information security while hiring new job candidates or examining the staff is justified. Based on the Russian Federation Constitution and the Labour Codex we justify the legality of the use of the polygraph in Russian Federation. Based on the theoretical approach describing the freeze-flight-fight reaction, as well as the Ivanitsky's theory of informational synthesis we justified the scientific value of psychophysiological methods of detecting lies. In order to justify a reliability of the obtained information we make use of statistical studies by American scientists. A list of information needed to identify insider threats and incident investigation is given in this paper, and it is proposed to use the polygraph in order to obtain this information directly from those who obtain it.

Keywords: insider threat to information security, polygraph, polygraph verification, validity of verification, scientific character of method, reliability of information.
For citation. **OBUKHOV, Alexandr Nikolaevich.** On the use of polygraph in the interests of identifying insider threats to information security. IT Security, [S.l.], v. 24, n. 3, p. 60-66, july 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/265>. Date accessed: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.07.

Информатизация общества, сопровождающаяся резким ростом стоимости информации, собираемой, хранимой, обрабатываемой и передаваемой информационными системами, привела к необходимости развития систем защиты информации. На сегодняшний день системы защиты информации, в условиях конфликта с системами несанкционированного доступа к информации, получили широкое распространение и непрерывно развиваются. Однако, одной из наиболее актуальных проблем современной информационной безопасности продолжает оставаться проблема выявления внутреннего нарушителя – инсайдера, как среди кандидатов на работу, так и среди работающего персонала организации. В этой связи целью статьи является обоснование целесообразности, законности, научности и точности применения психофизиологического метода выявления лжи в интересах выявления инсайдерских угроз информационной безопасности.

В зависимости от мотивации выделяют следующие группы внутренних нарушителей [1]:

- немотивированные;
- обиженные;
- нелояльные;
- специально внедренные.

При этом немотивированные включают в себя халатных и манипулируемых (под воздействием методов социальной инженерии), а специально внедренные - тех, кто планирует уволиться после совершения нарушения, и тех, кто планирует длительно работать в организации.

Ключевую роль в противодействии инсайдерам играет служба безопасности организации, на которую возлагаются задачи:

- недопущение в организацию специально внедряемых лиц;
- выявление ранее специально внедрённых лиц;
- выявление нелояльных и обиженных лиц;
- выявление немотивированных нарушителей;
- расследование инцидентов;
- профилактика внутренних нарушений.

Решение вышеназванных задач обусловливает необходимость ведения работы с кандидатами на работу и с работающим персоналом с целью получения сведений о факторах риска и деятельности, которая наносит или может нанести ущерб организации.

В частности, при подборе кадров в интересах выявления специально внедряемых лиц, а также негативно мотивированных и потенциально проблемных лиц, до принятия решения о приёме на работу и допуске к информационным ресурсам организации, необходимо выяснить такие сведения о кандидате, как

- наличие негативных мотивов устройства на работу в организацию;
- наличие связи с конкурентами (противником), преступной средой;
- наличие судимостей, долгов (в т.ч. больших кредитов), алкогольной, игровой и иных зависимостей;
- причастность к совершению преступлений, правонарушений;
- употребление наркотиков и психотропных средств;

- наличие проблем на предыдущих местах работы, увольнение по негативным мотивам;
- наличие дополнительных доходов и незаконных вознаграждений на предыдущих местах работы и др.

При работе с работающим персоналом в ходе плановых (профилактических) проверок и при назначении на отдельные должности, также необходимо своевременно получать сведения о факторах риска и о совершенных действиях, опасных или потенциально опасных для организации, таких как:

- появление (наличие) негативных мотивов при работе в организации, снижение лояльности;
- появление (наличие) связи с конкурентами (противником), преступной средой;
- появление (наличие) судимостей, долгов (в т.ч. больших кредитов), алкогольной, игровой и иных зависимостей;
- причастность к совершению преступлений, правонарушений;
- употребление наркотиков и психотропных средств;
- нарушение требований законов, локальных нормативных актов, трудового договора, инструкций и т.п.;
- передача (обсуждение) сведений, составляющих государственную, служебную, коммерческую и иную тайну, посторонним лицам;
- наличие дополнительных доходов и незаконных вознаграждений (в т.ч. за информацию) и т.п.

При проведении служебных разбирательств (внеплановых проверок) по выявленным инцидентам необходимо получение сведений о сотрудниках организации в части

- их причастности к расследуемому событию;
- наличия у них знаний о расследуемом событии.

Очевидно, что получить вышеперечисленные сведения в полном объёме возможно только непосредственно от самих кандидатов на работу и работающих сотрудников. Однако проведение бесед, анкетирование и приём заявлений не гарантируют получение достоверной информации.

Для получения достоверных сведений в интересах выявления и пресечения инсайдерских нарушений возможно проведение организационно-технического мероприятия – проверки с применением полиграфа (ППП). Также это мероприятие известно, как опрос с использованием полиграфа (ОИП), специальное психофизиологическое исследование (СПФИ), тестирование на полиграфе (ТнП).

Проверка с применением полиграфа – это мероприятие (процедура), имеющее целью получение от проверяемого лица сведений по интересующим работодателя вопросам и проверку их достоверности. Для достижения этой цели с проверяемым лицом проводится беседа по существу проводимой проверки, а достоверность или правдивость предоставленных сведений оценивается с применением полиграфа в результате сравнения реакций организма проверяемого лица на задаваемые вопросы различной смысловой направленности.

Полиграф – это техническое устройство, предназначенное для одновременной регистрации нескольких физиологических показателей организма человека и их изменений, возникающих в результате последовательного предъявления стимулов различного вида: вопросов, фотографий, предметов. Наибольшее распространение получили полиграфы, регистрирующие такие физиологические показатели организма проверяемого лица, как частота и глубина дыхания, частота сердечных сокращений и кровенаполнение сосудов и капилляров, величина кожной реакции.

Применение полиграфа, несмотря на многолетнюю историю метода инструментальной детекции лжи по изменениям физиологических параметров, традиционно вызывает вопросы о законности проведения проверки, научности метода и точности получаемых результатов.

Говоря о законности проведения ППП в интересах выявления и пресечения инцидентов с инсайдерами, следует отметить следующее.

Основной Закон Российской Федерации «Конституция Российской Федерации» [2] определяет, что «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ст. 29). Вместе с тем, никто не должен подвергаться пыткам, насилию, другому жестокому или унижающему его достоинство обращению или наказанию, никто не может быть без добровольного согласия подвергнут медицинским, научным или иным опытам (ст. 21).

В соответствии с Трудовым кодексом [3], все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (ст.86).

Именно требования ст. 21 Конституции РФ и ст.86 Трудового Кодекса, а также тот факт, что применение полиграфа предполагает установку датчиков на проверяемых лиц, что не может быть осуществлено негласно, без их согласия, определили основной принцип проведения ППП - *добровольность* процедуры, подтверждаемая письменным согласием.

Но при этом Трудовым Кодексом закреплено право работодателя разрабатывать и реализовывать локальные нормативные акты (ст.8). На основании этого положения работодатель может разрабатывать акты (инструкции), регламентирующие применение полиграфа в организации в отношении кандидатов на работу и работающего персонала. Обязательность прохождения полиграфа, как правило, закрепляется в трудовом договоре, а также в должностных инструкциях. Отказ от прохождения ППП без уважительной причины равносилен несоблюдению условий трудового договора и должностных инструкций, что может стать основанием для увольнения (ст.81, п.13).

Говоря о научности метода, следует отметить следующее.

Проверка с применением полиграфа является одним из прикладных направлений *психофизиологии*, раздела психологии, в котором изучается изменение различных физиологических показателей человека (таких как электрическое сопротивление кожи, частота сердечных сокращений, частота и глубина дыхания) в зависимости от психологического состояния.

В течение 140-летней истории практического применения психофизиологического метода выявления лжи с использованием технических устройств учёные неоднократно предпринимали попытки дать естественно-научное объяснение и теоретическое обоснование тех сложных процессов, которые происходят в психике человека и его организме и приводят к возможности выявления у человека скрываемой им информации в ходе проверки на полиграфе.

На сегодняшний день существует ряд теоретических концепций, с различной степенью успешности объясняющих, каким образом с помощью полиграфа удается выявить ложь [4, 5, 6]: теория угрозы наказания; теория конфликта; условно-рефлекторная теория; теория активации; информационная теория П.В. Симонова; теория информационного синтеза А.М. Иваницкого; теория целенаправленного тестирования памяти Ю.И. Холодного и др.

В настоящее время наиболее популярной теорией, дающей естественно-научное объяснение психофизиологического метода выявления лжи, является *теория о реакции замирания/бегства/борьбы*, суть которой состоит в том, что при возникновении опасности

в организме человека возникает рефлекторная (бессознательная) реакция, направленная на его спасение.

В дикой природе при появлении хищника человек рефлекторно замирает. Это необходимо для того, чтобы движениями не привлекать к себе внимания, стать незаметным (слиться с окружающей средой), обдумать последующие действия. Если остаться незамеченным не удалось, первейшее действие – покинуть опасное место, то есть бегство. Если бегство невозможно, тогда – борьба за выживание. Все эти проявления реакции замирания/бегства/борьбы сопровождаются значительными изменениями в функционировании всех физиологических систем организма. В частности, в сердечно-сосудистой системе наблюдается изменение частоты сердечных сокращений, кровенаполнения сосудов; в дыхательной - изменение частоты и глубины дыхания; в коже - потовыделение и др.

В ходе ППП для причастного к проверяемому событию (фактору риска) лица опасность представляют задаваемые вопросы и, несмотря на то, что проверяемый не может ни уйти, ни вступить в борьбу, его организм реагирует всеми физиологическими системами, что и регистрирует полиграф.

Для научного обоснования психофизиологического метода выявления лжи интересна разработанная в 70-х годах прошлого века теория информационного синтеза А.М. Иваницкого [7], лежащая в основе одного из основных законов психофизиологии – *закона силы,* согласно которому, чем сильнее раздражение, тем более выражена ответная реакция организма. Применительно к проверке с применением полиграфа закон силы определяет, что увеличение психофизиологических реакций опрашиваемого лица на тот или иной стимул (вопрос) является свидетельством субъективной значимости этого стимула.

Любой человек, подвергаемый проверке на полиграфе, независимо от того, скрывает он информацию о расследуемом событии или не скрывает, испытывает потребность в безопасности, поскольку боится либо разоблачения, либо ошибочного решения. Потребность в безопасности формирует соответствующую мотивацию. В качестве регулирующего механизма мотивации выступают эмоции, при этом сила проявления эмоций обратно пропорциональна объёму имеющейся информации о способе удовлетворения испытываемой потребности. Таким образом, значимость стимула в условиях ППП определяется возможностью удовлетворения потребности в безопасности [6].

Последовательность событий в мозговых структурах при ППП можно представить следующим образом [6]. Сенсорные системы производят анализ физических характеристик стимула (вопроса) и передают соответствующую информацию в проекционную область коры, где на основе последующего синтеза возникает отраженный образ внешнего стимула. Далее происходит сравнение физических характеристик стимула с хранящимися в фенотипической памяти следами раздражений, оставленными прошлыми событиями. При их совпадении происходит активация следов памяти, и возбуждение по нисходящим путям переходит на соответствующие центры эмоций и мотиваций организма, т.е. на структуры подбугорной области и лимбической системы, которые включают необходимые вегетативные реакции [7].

Из сказанного следует, что наличие или отсутствие в памяти информации об интересующем событии является той характеристикой памяти проверяемого лица, которая, взаимодействуя с эмоциональными и мотивационными механизмами, определяет уровень значимости и формирует дифференцированное проявление вегетативных ответов на стимулы. Если в памяти имеется информация об интересующем событии прошлого, реакции будут более сильные, если такой информации в памяти нет – менее сильные. Схематично это можно отобразить в виде структурных формул:

- у «причастного»: $P_{\text{сильн.}} = З_{\text{бол.}} = (П + И_{\text{соб.}}) \times (Э + М)$;
- у «непричастного»: $P_{\text{слаб.}} = З_{\text{мен.}} = П \times (Э + М)$,

где P – вегетативная реакция (сильная или слабая), З – значимость (большая или меньшая), П – фенотипическая память, $И_{\text{соб.}}$ – информация об интересующем событии прошлого, Э – эмоции, М – мотивация [6].

Из сказанного видно, что на величину регистрируемых в ходе ППП реакций влияет большое количество факторов: потребность в безопасности, мотивированность и эмоциональность (в первую очередь тревожность) опрашиваемого лица, а также наличие в памяти информации о расследуемом и аналогичных событиях. Всё это конечно же может привести к ошибкам при принятии решения специалистом-полиграфологом. В связи с этим, проводя ППП, необходимо помнить, что результаты проверки носят вероятностный характер и могут быть использованы как ориентирующие.

Говоря о точности получаемых результатов или достоверности проверяемой информации, следует отметить, что точность зависит от многих факторов: профессионального уровня специалиста-полиграфолога, валидности применяемых методик, качества полиграфа, индивидуальных особенностей опрашиваемого лица, внешних (отвлекающих) факторов и т.п.

Статистические исследования, проведенные в США, позволили получить зависимости точности ряда методик от результатов тестирования [8]. Это в свою очередь позволило определить «пороги» для принятия решения с заданной точностью. Выявлен целый ряд методик, позволяющих получать результат с точностью 0,9 и выше при проведении проверок с применение полиграфа в течении 2,5-4 часов.

Таким образом, на сегодняшний день полиграфолог имеет возможность выбрать наиболее «точную» методику и по результатам тестирования может ответить на вопросы:

1. Какова достоверность предоставленной информации?
2. Соответствует ли предоставленная информация заданной достоверности (например, 0,95) или нет?

(Конечно же эти результаты приблизительны. Для получения более точных результатов необходимо проведение аналогичного исследования в России на русском языке.)

Таким образом, в статье показана возможность и целесообразность проведения на законных основаниях проверок с применением полиграфа в отношении кандидатов на работу и работающего персонала с целью выявления инсайдерских угроз и расследования инцидентов, подтверждены их научность и высокая достоверность результатов.

СПИСОК ЛИТЕРАТУРЫ

1 Зайцев А.С., Малюк А.А. Исследование проблемы внутреннего нарушителя – М.: Вестник РГГУ. — 2012. —N 14. —С. 114–134.

2 Конституция Российской Федерации. – М.: Юрид.лит., 1993.

3 Трудовой кодекс Российской Федерации от 30дек. 2001 г. №197ФЗ.

4 Холодный Ю.И. Опрос с использованием полиграфа и его естественно-научные основы. Полиграф в России: 1993-2008: Ретроспект. сб. статей. Авт.-сост. Ю.И. Холодный. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 177 с.

5 Обухов А.Н., Обухова И.П. Теоретические и методические основы применения полиграфа. Учебное пособие. – 5-е изд. – М: ДГСК МВД России, 2015. – 272 с.

6 Иванов Р.С. «Закон силы» в ситуации психофизиологического исследования с применением полиграфа. Научный журнал «Вестник психофизиологии». №2, 2016. С.12-21.

7 Иваницкий А.М. Мозговые механизмы оценки сигналов – М.: «Медицина» – 1976. – 298 с.

8 Donald J.Krapohl, Pamela K. Show «Fundamentals of Polygraph Practice» Academic Press, 2015, 364 p.

REFERENCES:

1. Zaitsev A.S., Maluk A.A. The study of the problem of domestic intruder. – M.: Vestnik RGGU. - 2012. - N 14. —P. 114–134. (in Russian).
2. Konstitutsiya Rossiyskoy Federatsii. – M.: Yurid.lit., 1993.
3. Trudovoy kodeks Rossiyskoy Federatsii ot 30 dek. 2001 g. №197FZ.
4. Kholodny Yu.I. A survey using polygraph and its scientific basis. Poligraf v Rossii: 1993-2008: Retrospekt. sb. Statey Avt.-cost. Yu.I. Kholodny, - M.: Izd-vo MGTU im. N.E.Baumana, 2008. - 177 p. (in Russian).
5. Obukhov A.N., Obukhova I.P. Theoretical and methodological basis for the use of the polygraph. Uchebnoe posobie: - 5-e izd. – M: DGSK MVD Rossii, - 272 p. (in Russian).
6. Ivanov R.S. The "law of force" in a situation of psychophysiological research using the polygraph. Nauchny zhurnal “Vestnik psihofiziologii”. № 2, 2016. S.12-21. (in Russian).
7. Ivanitsky A.M. Brain mechanisms for the evaluation of signals – M.:”Meditsina” – 1976. – 298 p. (in Russian).
8. Donald J.Krapohl, Pamela K. Show «Fundamentals of Polygraph Practice» Academic Press, 2015, 364 p.