Морозова Татьяна Романовна,
доктор психологических наук, профессор,
аттестованный судебный эксперт,
президент Всеукраинской ассоциации полиграфологов

Методика выявления скрываемой информации: расследование несанкционированного проникновения в электронную систему компании

Уже десятки лет бизнес, независимо от его размера и уровня технологичности, невозможно представить без использования программного обеспечения — как общераспространенного, так и разработанного специально под потребности и по заказу конкретной компании. Однако развитие технологий не дало бизнесменам желаемой информационной защиты, скорее наоборот: та финансовая информация, которую раньше приходилось собирать по крупицам, с привлечением агентурного аппарата и риском его разоблачения, сейчас может быть похищена за один или несколько несанкционированных входов благодаря менеджеру среднего звена, который элементарно не настроил двухфакторную аутентификацию. Те суммы, которые раньше вор похищал физически из сейфа, рискуя быть обнаруженным на месте совершения преступления, зафиксированным камерами видеонаблюдения, зачастую ничтожны по сравнению с деньгами, которые выводит хакер электронным способом, находясь при этом за тысячи километров от жертвы преступления. Те массивы компромата на компанию, для получения которых когда-то требовалось привлекать группу частных детективов/расследователей, чья активность не могла оставаться долго незамеченной, сейчас могут быть скачаны в течение одной ночи, но при этом нанести бизнесу сокрушительный удар, сделать его заложником вымогателей и шантажистов [1].

Вместе с тем, есть вещи, которые остаются неизменными:

– преступления планируют и реализуют конкретные люди;

– для реализации преступного замысла необходимо как минимум воспользоваться уязвимостью электронной системы, которая может быть в том числе мастерски замаскирована под банальную халатность конкретного сотрудника;

– сотрудники, нелояльные к компании, те, кто не разделяет ее ценностей и не чувствует внутренней вовлеченности в команду и общее дело, априори склонны к саботажу инструктажей по информационной безопасности, и их бездействие не менее опасно, чем спланированные вредительские действия;

– фаворитизм, подбор специалистов, отвечающих за кибербезопасность, по принципу личного удобства для руководителей среднего звена, а не на основании профессионализма, рано или поздно заканчивается для компании потерей данных, денег или же репутации.

Анализ 41 полиграфологического исследования, проведенного в 2025–2026 гг. с помощью методики выявления скрываемой информации (МВСИ) в рамках служебных расследований по фактам несанкционированного проникновения во внутренние системы трех разных компаний, позволил определить обязательные составляющие тестовых опросников, разработанных для таких случаев. Безусловно, каждая ситуация имела свои отличия, в частности отличались способы обхода существующих в компаниях систем защиты информации и конечные последствия инцидентов: в одних случаях это была выгрузка компрометирующей информации на внешние ресурсы, в других – вывод денежных средств и т. д. Однако было и много общего в развитии чрезвычайного происшествия, а что касается заказчиков – они были практически единодушны как в своих подозрениях и опасениях, так и в содержании вопросов, вынесенных на разрешение специалиста.

Обобщение результатов успешно проведенных тестирований, которые, помимо прочего, впоследствии получили подтверждение со стороны независимого технического аудита, показывает, что в третьем блоке таких опросников должны быть предусмотрены вопросы, позволяющие установить у респондента следующее:

1) осведомленность респондента-сотрудника компании относительно лиц, причастных к атаке на компанию.

С этой целью могут быть использованы тесты проверки версий вроде «Известно ли Вам, что на самом деле происходи?», «Известно ли вам, кто на самом деле атакует Компанию?», «Что из перечисленного касается вас лично?», с оформлением просоциальной версии респондента в вопросах: «Компанию атаковала группа неизвестных лично вам людей?», «Компанию атаковала группа людей, о которых вы ничего не знаете?», «Вы действительно не знаете, кто атаковал компанию» [2, 3].

Примеры тестов и полиграмм к ним приведены ниже на рис. 1.1–1.3.1;

Тест 1 | Тест 2 | **Тест 3** | Тест 4 | Тест 5 | Тест 6 | Тест 7 | Тест 8 | Тест 9 | Тест 10 |

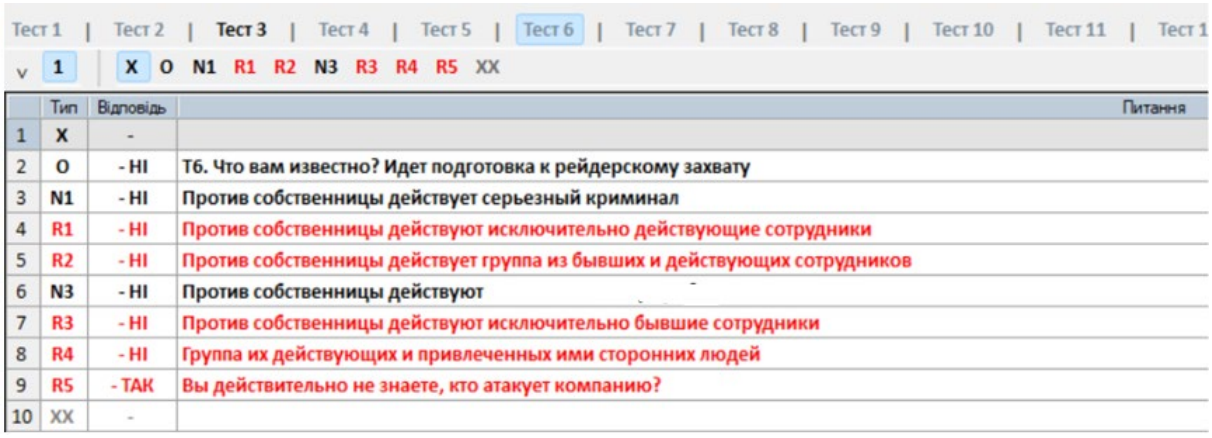
v 1 | X O N1 R1 R2 N3 R3 R4 R5 XX

	Тип	Відповідь	
1	X	-	
2	O	- Н / З	Т6. Что в действительности происходит? Идет подготовка к рейдерскому захвату
3	N1	- Н / З	Против собственницы действует серьезный криминал
4	R1	- Н / З	Против собственницы действуют исключительно действующие сотрудники
5	R2	- Н / З	Против собственницы действует группа из бывших и действующих сотрудников
6	N3	- Н / З	Против собственницы действуют спецслужбы
7	R3	- Н / З	Против собственницы действуют исключительно бывшие сотрудники
8	R4	- Н / З	Группа их действующих и привлеченных ими сторонних людей
9	R5	- ТАК	Группа людей, о которых вы ничего не знаете
10	XX	-	

Рис. 1.1



Рис. 1.1.1



	Тип	Відповідь	Питання
1	X	-	
2	O	- HI	Тб. Что вам известно? Идет подготовка к рейдерскому захвату
3	N1	- HI	Против собственницы действует серьезный криминал
4	R1	- HI	Против собственницы действуют исключительно действующие сотрудники
5	R2	- HI	Против собственницы действует группа из бывших и действующих сотрудников
6	N3	- HI	Против собственницы действуют
7	R3	- HI	Против собственницы действуют исключительно бывшие сотрудники
8	R4	- HI	Группа их действующих и привлеченных ими сторонних людей
9	R5	- ТАК	Вы действительно не знаете, кто атакует компанию?
10	XX	-	

Рис. 1.2

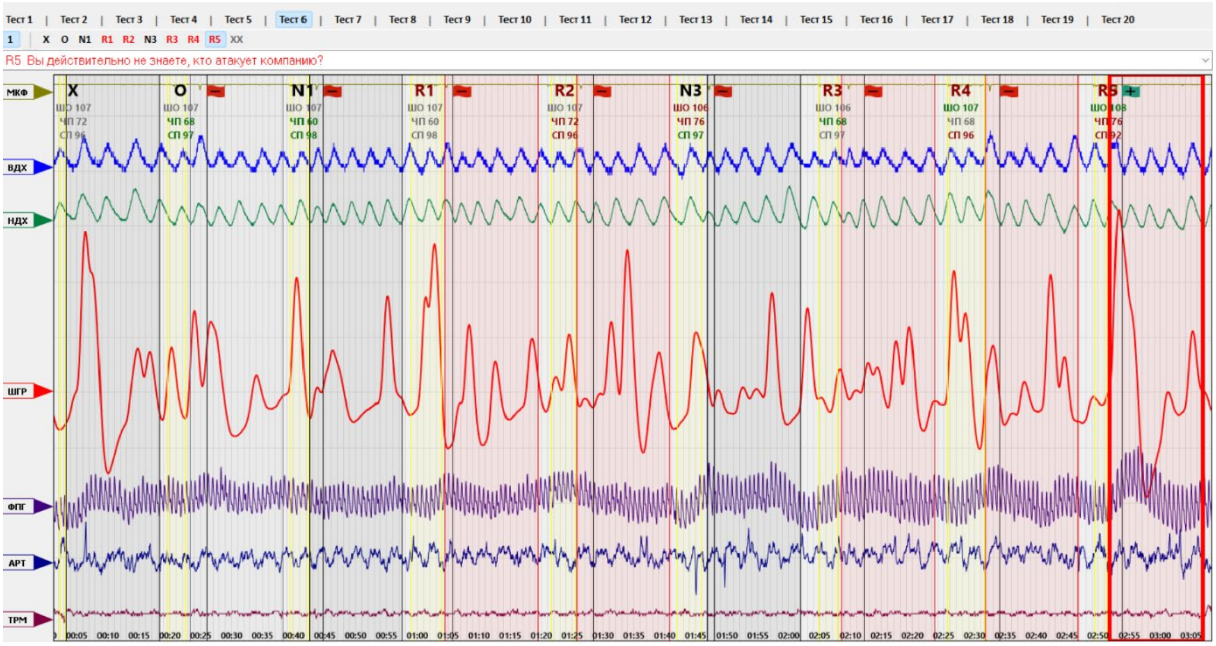
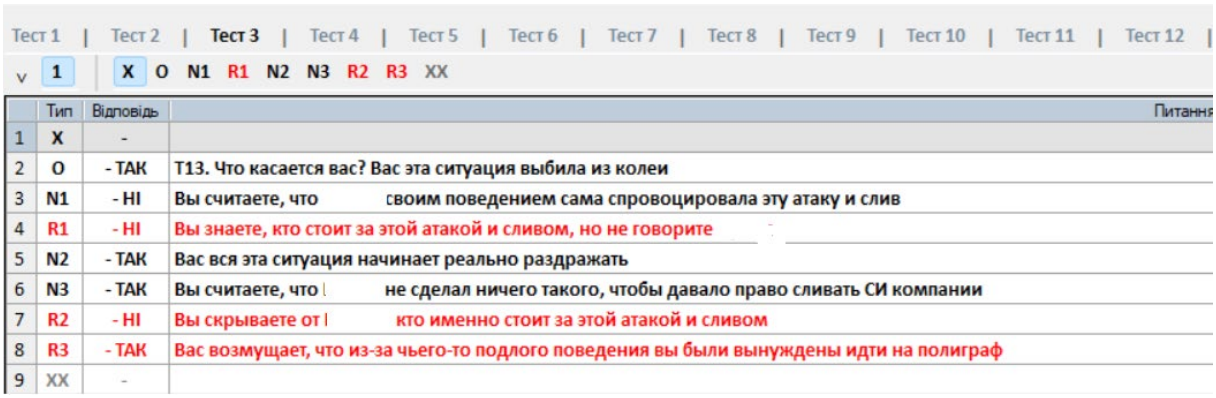


Рис. 1.2.1



	Тип	Відповідь	Питання
1	X	-	
2	O	- ТАК	Т13. Что касается вас? Вас эта ситуация выбила из колеи
3	N1	- НІ	Вы считаете, что своим поведением сама спровоцировала эту атаку и слив
4	R1	- НІ	Вы знаете, кто стоит за этой атакой и сливом, но не говорите
5	N2	- ТАК	Вас вся эта ситуация начинает реально раздражать
6	N3	- ТАК	Вы считаете, что не сделал ничего такого, чтобы давало право сливать СИ компании
7	R2	- НІ	Вы скрываете от кто именно стоит за этой атакой и сливом
8	R3	- ТАК	Вас возмущает, что из-за чьего-то подлого поведения вы были вынуждены идти на полиграф
9	XX	-	

Рис. 1.3

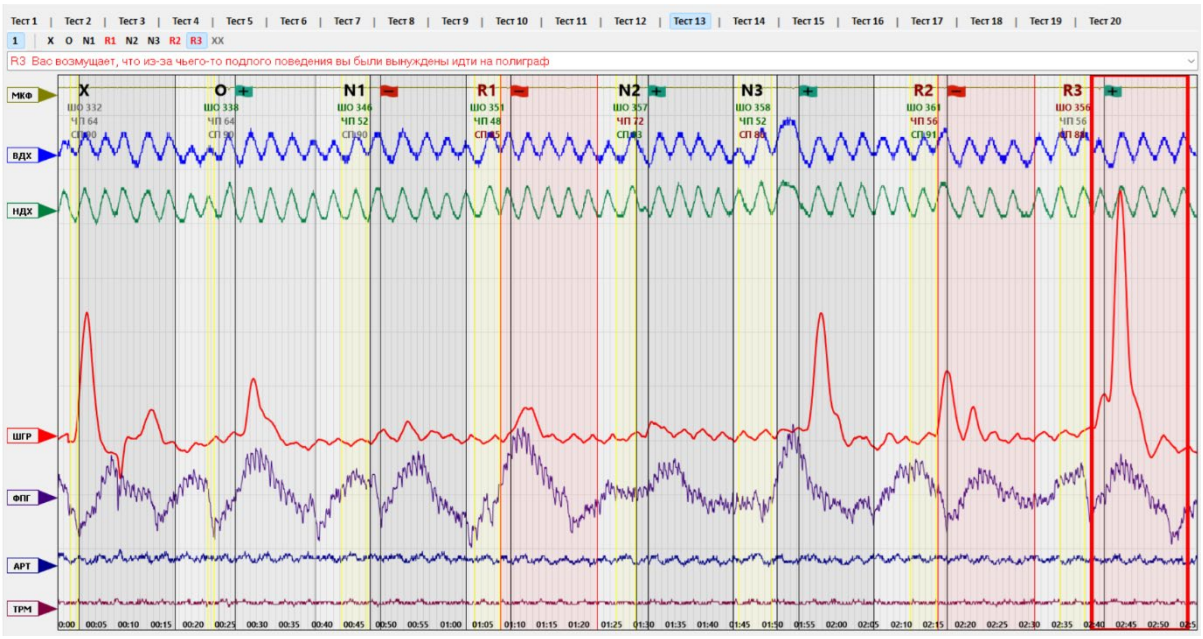


Рис. 1.3.1

2) **лояльность/нелояльность респондента-сотрудника компании по отношению к компании, руководству:** равнодушие, внутренняя поддержка атаки, восприятие ее как допустимого способа сведения счетов с руководством, либо осуждение атаки, переживание за возможные негативные последствия для компании.

С этой целью могут быть использованы тесты проверки версий вроде «Кто вы, реально в ситуации атаки на компанию?», «Ваше отношение к атаке на компанию?» с вопросами-версиями респондентов, озвученными ими в предтестовой и межтестовых беседах.

Примеры тестов и полиграмм к ним приведены ниже на рис. 2.1–2.3.1;

Тест 1 | Тест 2 | **Тест 3** | Тест 4 | Тест 5 | Тест 6 | Тест 7 | Тест 8 | Тест 9 | Тест 10 | Тест 11

v **1** | **X** O N1 R1 N2 R2 N3 R3 XX

	Тип	Відповідь	
1	X	-	
2	O	- Н / З	Т8. Кто вы, реально, во всей этой ситуации? Вы человек, чья фамилия всплыла в слитых файлах
3	N1	- ТАК	Вы в окружении сотрудников анализировали, кто мог отомстить [redacted]
4	R1	- НІ	Вы в числе тех, кто ждет, когда у компании возникнут серьезные проблемы
5	N2	- ТАК	Вы ощущаете злость к людям, заварившим всю эту кашу
6	R2	- НІ	Вы являетесь глазами и ушами людей, атакующих компанию
7	N3	- Н / З	Вы боитесь из-за этой ситуации потерять нормальную работу
8	R3	- ТАК	Необоснованно подозреваемая
9	XX	-	

Рис. 2.1

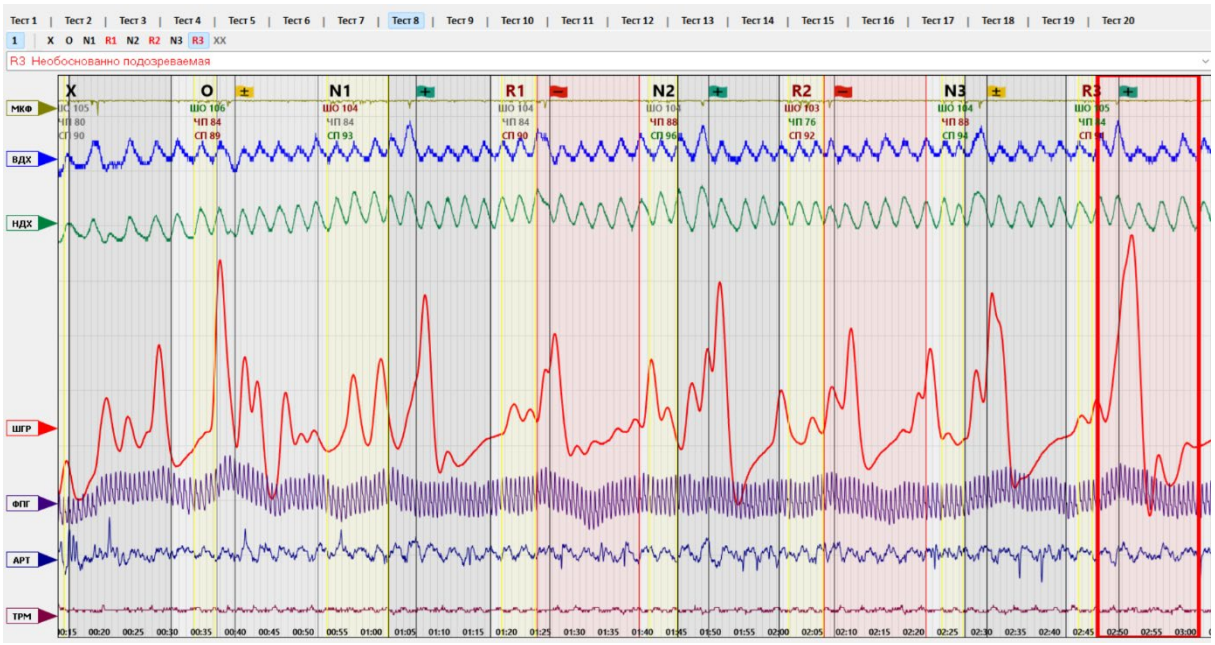
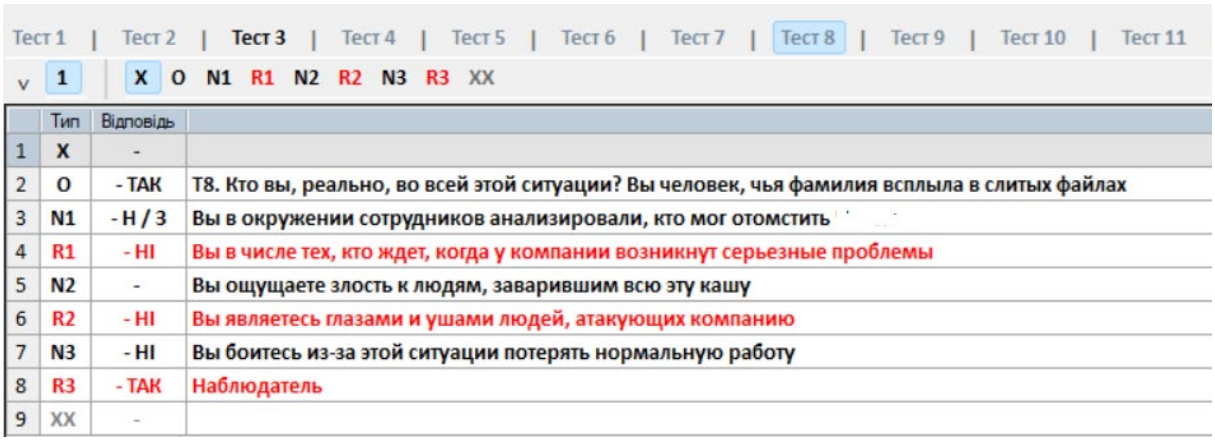


Рис. 2.1.1

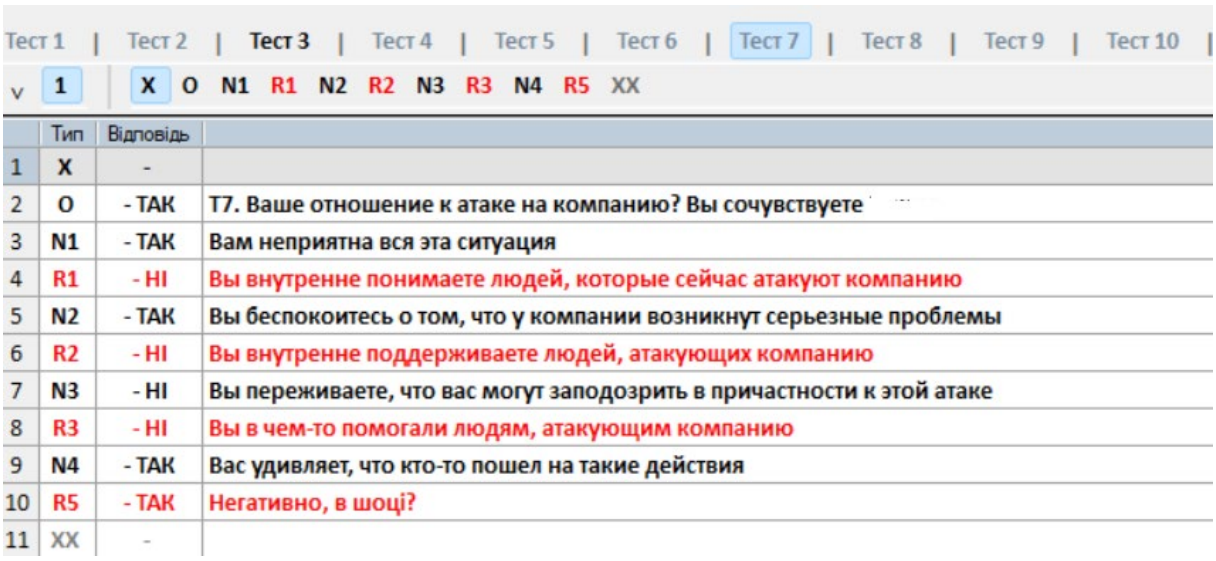


	Тип	Відповідь	
1	X	-	
2	O	- ТАК	Т8. Кто вы, реально, во всей этой ситуации? Вы человек, чья фамилия всплыла в слитых файлах
3	N1	- Н / З	Вы в окружении сотрудников анализировали, кто мог отомстить
4	R1	- НІ	Вы в числе тех, кто ждет, когда у компании возникнут серьезные проблемы
5	N2	-	Вы ощущаете злость к людям, заварившим всю эту кашу
6	R2	- НІ	Вы являетесь глазами и ушами людей, атакующих компанию
7	N3	- НІ	Вы боитесь из-за этой ситуации потерять нормальную работу
8	R3	- ТАК	Наблюдатель
9	XX	-	

Рис. 2.2



Рис. 2.2.1



	Тип	Відповідь	
1	X	-	
2	O	- ТАК	Т7. Ваше отношение к атаке на компанию? Вы сочувствуете
3	N1	- ТАК	Вам неприятна вся эта ситуация
4	R1	- НІ	Вы внутренне понимаете людей, которые сейчас атакуют компанию
5	N2	- ТАК	Вы беспокоитесь о том, что у компании возникнут серьезные проблемы
6	R2	- НІ	Вы внутренне поддерживаете людей, атакующих компанию
7	N3	- НІ	Вы переживаете, что вас могут заподозрить в причастности к этой атаке
8	R3	- НІ	Вы в чем-то помогали людям, атакующим компанию
9	N4	- ТАК	Вас удивляет, что кто-то пошел на такие действия
10	R5	- ТАК	Негативно, в шоці?
11	XX	-	

Рис. 2.3

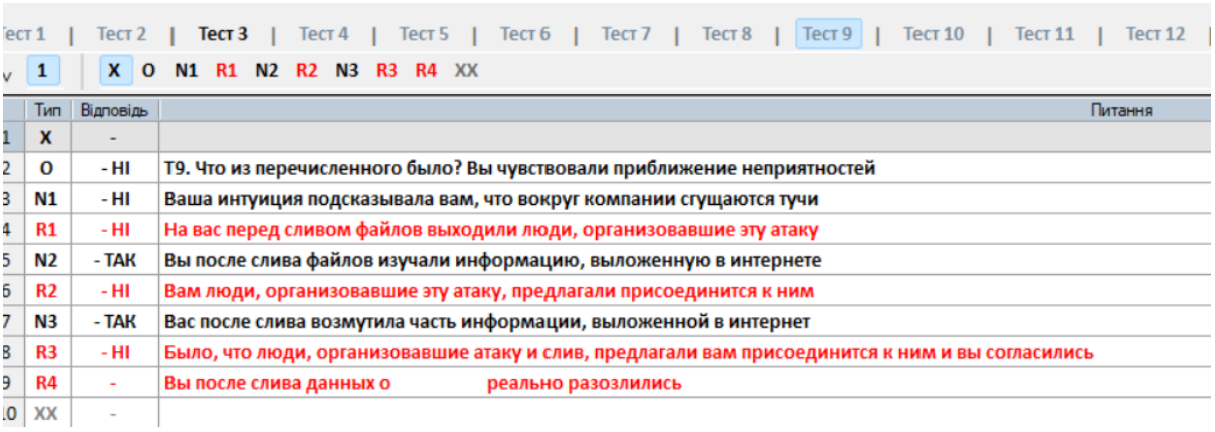


Рис. 2.3.1

3) привлечение респонедента-сотрудника компании организаторами атаки к ее осуществлению.

С этой целью могут быть использованы тесты на знание неизвестного решения вроде «Что именно из переличисленного происходило лично с вами?», с помощью которых выясняется, контактировали ли причастные к атаке с респондентом, предлагали ли присоединиться к ним, принял ли он это предложение; принимал ли он участие в планировании и обсуждении атаки? [2, 3].

Примеры тестов и полиграмм к ним приведены ниже на рис. 3.1–3.2.1;

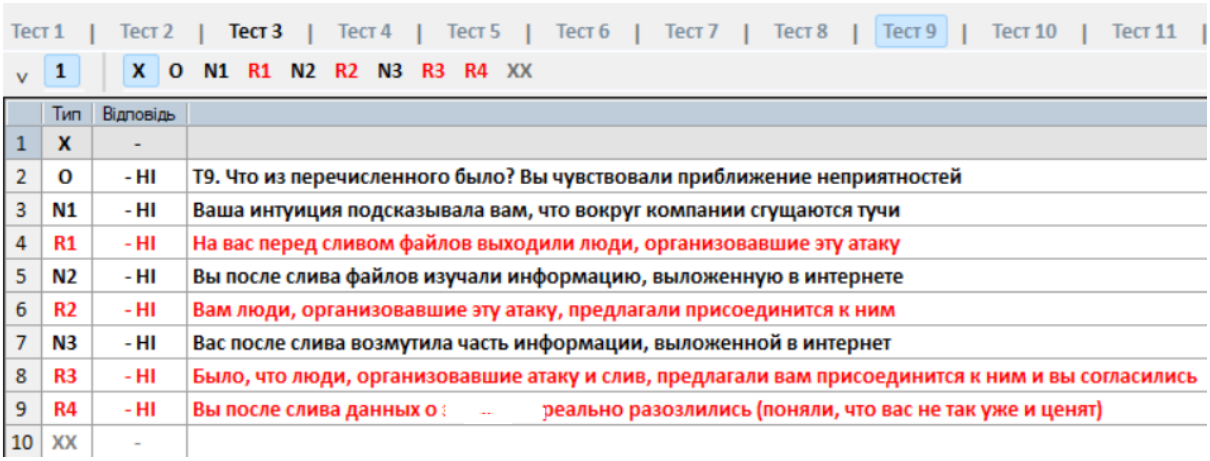


	Тип	Відповідь	Питання
1	X	-	
2	O	- НІ	Т9. Что из перечисленного было? Вы чувствовали приближение неприятностей
3	N1	- НІ	Ваша интуиция подсказывала вам, что вокруг компании сгущаются тучи
4	R1	- НІ	На вас перед сливом файлов выходили люди, организовавшие эту атаку
5	N2	- ТАК	Вы после слива файлов изучали информацию, выложенную в интернете
6	R2	- НІ	Вам люди, организовавшие эту атаку, предлагали присоединится к ним
7	N3	- ТАК	Вас после слива возмутила часть информации, выложенной в интернет
8	R3	- НІ	Было, что люди, организовавшие атаку и слив, предлагали вам присоединится к ним и вы согласились
9	R4	-	Вы после слива данных о реально разозлились
10	XX	-	

Рис. 3.1



Рис. 3.1.1



	Тип	Відповідь	
1	X	-	
2	O	- HI	Т9. Что из перечисленного было? Вы чувствовали приближение неприятностей
3	N1	- HI	Ваша интуиция подсказывала вам, что вокруг компании сгущаются тучи
4	R1	- HI	На вас перед сливом файлов выходили люди, организовавшие эту атаку
5	N2	- HI	Вы после слива файлов изучали информацию, выложенную в интернете
6	R2	- HI	Вам люди, организовавшие эту атаку, предлагали присоединится к ним
7	N3	- HI	Вас после слива возмутила часть информации, выложенной в интернет
8	R3	- HI	Было, что люди, организовавшие атаку и слив, предлагали вам присоединится к ним и вы согласились
9	R4	- HI	Вы после слива данных о [illegible] реально разозлились (поняли, что вас не так уже и ценят)
10	XX	-	

Рис. 3.2



Рис. 3.2.1

4) инициирование респондентом-сотрудником компании атаки и привлечение к ней других лиц.

С этой целью могут быть использованы тесты на знание неизвестного решения вроде «Что из перечисленного происходило лично с вами?», с помощью которых выясняется, выходил ли респондент на кого-либо с предложением принять участие в атаке, получал ли он от кого-либо согласие на участие в ней; планировал ли, обсуждал ли атаку на этапе ее подготовки?

Примеры тестов и полиграмм к ним приведены ниже на рис. 4.1–4.2.1;

Тест 1 | Тест 2 | **Тест 3** | Тест 4 | Тест 5 | Тест 6 | Тест 7 | Тест 8 | Тест 9 | Тест 10 | Тест 11 | Тест 12

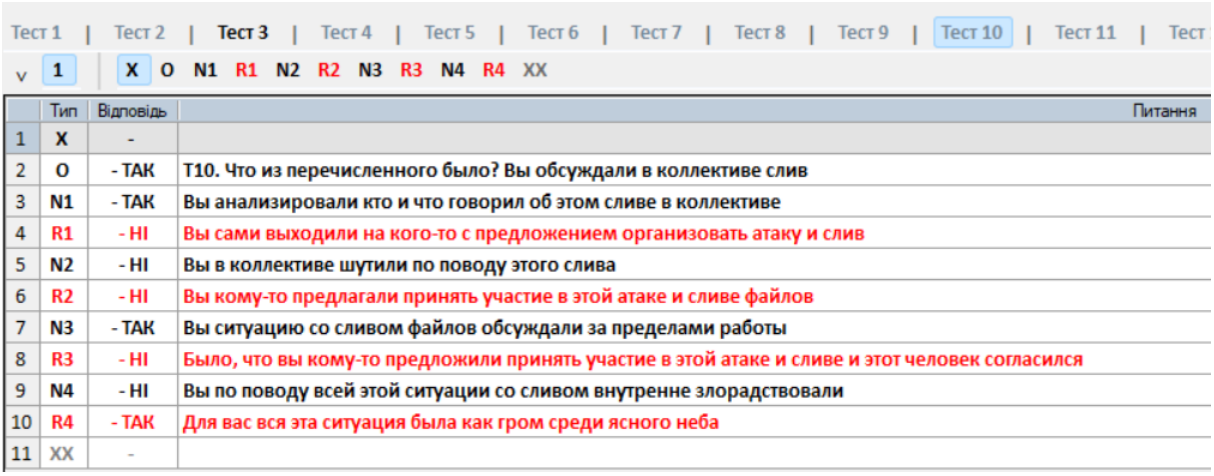
v 1 X O N1 R1 N2 R2 N3 R3 N4 R4 N5 R5 XX

	Тип	Відповідь	Питання
1	X	-	
2	O	- ТАК	T11. Какие факты имели место? Вы опаздывали на эту работу
3	N1	- НІ	Вы эту работу прогуливали
4	R1	- НІ	Вы до слива с кем-то обсуждали, как можно нанести компании ущерб
5	N2	- НІ	Вы на работе сплетничали
6	R2	- НІ	Вы до слива с кем-то обсуждали, как можно насолить собственнице
7	N3	- НІ	Вы внутри коллектива давали негативные характеристики
8	R3	- НІ	Вы с кем-то разрабатывали план мести компании и собственнице
9	N4	- ТАК	Вы на работе крыли матом
10	R4	- НІ	Вы с кем-то планировали месть компании и собственнице
11	N5	- НІ	Вы в рабочее время употребляли алкоголь
12	R5	- НІ	Вследствие вашего участия стала возможной эта атака на компанию
13	XX	-	

Рис. 4.1



Рис. 4.1.1



	Тип	Відповідь	Питання
1	X	-	
2	O	- ТАК	Т10. Что из перечисленного было? Вы обсуждали в коллективе слив
3	N1	- ТАК	Вы анализировали кто и что говорил об этом сливе в коллективе
4	R1	- НІ	Вы сами выходили на кого-то с предложением организовать атаку и слив
5	N2	- НІ	Вы в коллективе шутили по поводу этого слива
6	R2	- НІ	Вы кому-то предлагали принять участие в этой атаке и сливе файлов
7	N3	- ТАК	Вы ситуацию со сливом файлов обсуждали за пределами работы
8	R3	- НІ	Было, что вы кому-то предложили принять участие в этой атаке и сливе и этот человек согласился
9	N4	- НІ	Вы по поводу всей этой ситуации со сливом внутренне злорадствовали
10	R4	- ТАК	Для вас вся эта ситуация была как гром среди ясного неба
11	XX	-	

Рис. 4.2



Рис. 4.2.1

5) наличие у респондента-сотрудника компании коммуникации со злоумышленниками после совершения атаки.

С этой целью могут быть использованы тесты на знание неизвестного решения вроде «Что из перечисленного имело место?», с помощью которых выясняется, контактировал ли респондент с причастными к атаке после ее совершения, рассказывал ли им, какого психологического эффекта они достигли, каковы настроения в компании, как ведут себя и что говорят по поводу атаки руководители и сотрудники?

Примеры тестов и полиграмм к ним приведены ниже на рис. 5.1–5.1.1;

Тест 1 | Тест 2 | **Тест 3** | Тест 4 | Тест 5 | Тест 6 | Тест 7 | Тест 8 | Тест 9 | Тест 10 | Тест 11 | Тест 12

1 | X O N1 R1 N2 R2 N3 R3 N4 R4 N5 R5 XX

	Тип	Відповідь	Питання
1	X	-	
2	O	- НІ	Т12. Какие факты имели место? У вас на этой работе были конфликты
3	N1	- НІ	Вы на этой работе конфликтовали с другими сотрудниками
4	R1	- НІ	О настроениях в компании после слива рассказывали врагам компании
5	N2	- НІ	Вы на этой работе конфликтовали с руководством
6	R2	- НІ	Говорили причастным к атаке, что после слива говорили конкретные сотрудники
7	N3	- НІ	Вы на этой работе на других сотрудников перекидывали свою вину
8	R3	- НІ	Передавали причастным к атаке, что после слива говорила
9	N4	- НІ	Вас на этой работе кто-то подставлял
10	R4	- НІ	Обсуждали обстановку в компании после слива с причастными к атаке
11	N5	- ТАК	Вы в этой компании перекидывали свою работу на других
12	R5	- ТАК	Ви крили матом співробітників
13	XX	-	

Рис. 5.1



Рис. 5.1.1

6) сознательное игнорирование, невыполнение респондентом правил информационной безопасности.

Логично, что изначально необходимо выяснить с помощью отдельного теста, проводился ли с респондентом соответствующий инструктаж, какие именно из Доведенных предостережений/запретов он нарушил, а только затем – почему, по его мнению, стала возможной эта атака.

Примеры тестов и полиграмм к ним приведены ниже на рис. 6.1–6.2.1.

Тест 1 | Тест 2 | **Тест 3** | Тест 4 | Тест 5 | Тест 6 | Тест 7 | Тест 8 | Тест 9 | Тест 10 | Тест 11 | Тест 12 |

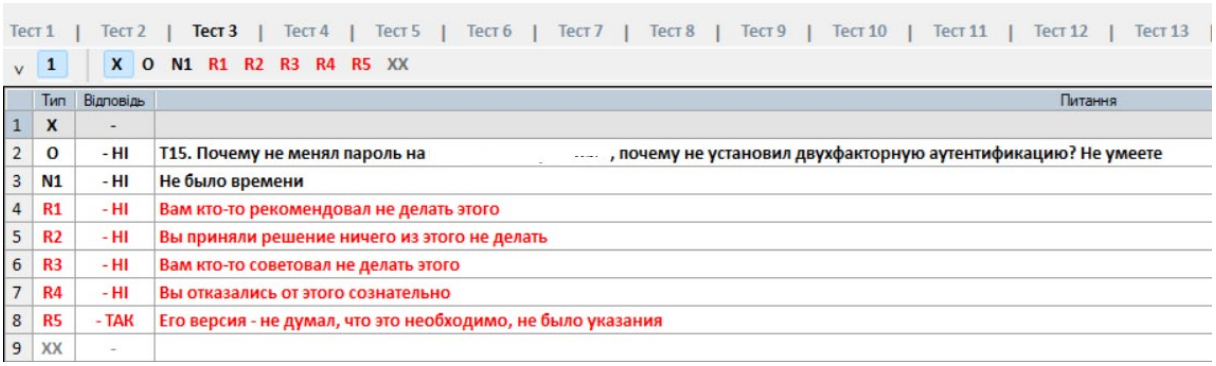
1 X O N1 R1 R2 R3 R4 R5 XX

	Тип	Відповідь	Питання
1	X	-	
2	O	- HI	T13. Что из перечисленного было? Вы забывал пароль входа в систему
3	N1	- HI	Вы сами заражали свой служебный ПК вирусами
4	R1	- HI	Вам на работе доводили сведения о потенциальных уязвимостях
5	R2	- HI	Вам на работе доводили требования информационной безопасности
6	R3	- HI	Вы на работе доводили принятые в компании процедуры предупреждения хакерских атак
7	R4	- HI	Вы знали все о том, как не стать жертвой хакерской атаки, однако проигнорировали правила безопасности
8	R5	- ТАК	Вам не хватало информации и знаний, как не стать жертвой хакерской атаки
9	XX	-	

Рис. 6.1



Рис. 6.1.1



	Тип	Відповідь	Питання
1	X	-	
2	O	- НІ	Т15. Почему не менял пароль на , почему не установил двухфакторную аутентификацию? Не умеете
3	N1	- НІ	Не было времени
4	R1	- НІ	Вам кто-то рекомендовал не делать этого
5	R2	- НІ	Вы приняли решение ничего из этого не делать
6	R3	- НІ	Вам кто-то советовал не делать этого
7	R4	- НІ	Вы отказались от этого сознательно
8	R5	- ТАК	Его версия - не думал, что это необходимо, не было указания
9	XX	-	

Рис. 6.2

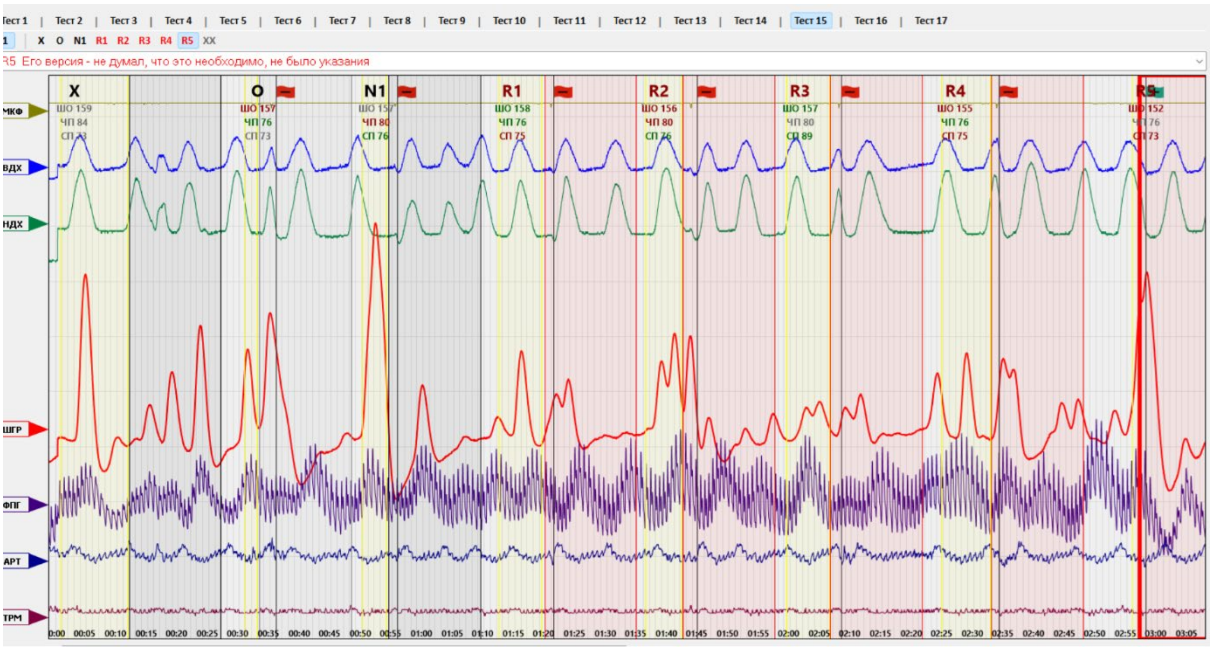
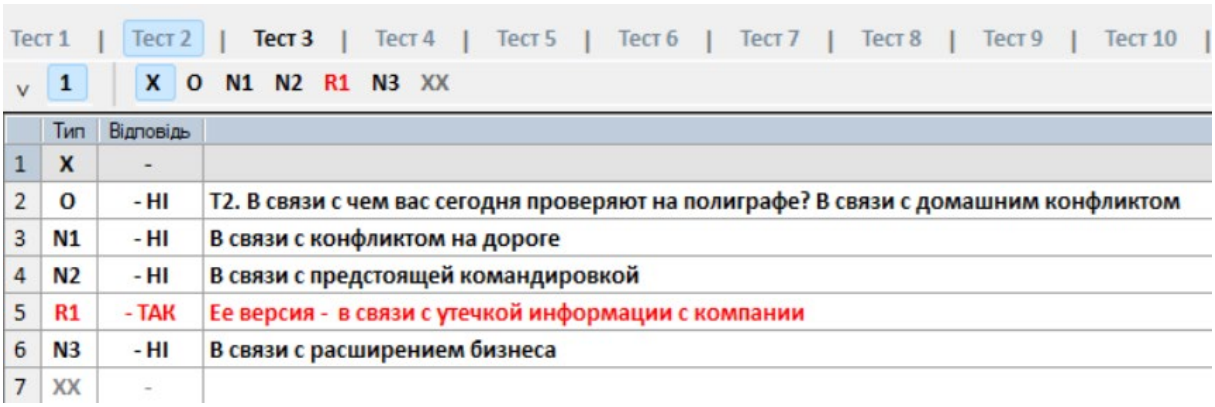


Рис. 6.2.1

Что касается стимульного, диагностического (тест Татьяны Кузьмич «Что вам абсолютно точно известно об атаке на компанию?») и четвертого блока тестовых опросников, предназначенных для использования в целях расследования несанкционированного проникновения в электронную систему компании, то они являются традиционными для МВСИ, а правила их формулирования подробно описаны в учебнике и монографии [2, 3].

Указанные тесты и полученные с их помощью полиграммы приведены на рис. 7.1–7.4.1.


Тест 1 | Тест 2 | Тест 3 | Тест 4 | Тест 5 | Тест 6 | Тест 7 | Тест 8 | Тест 9 | Тест 10

1 | X O N1 N2 R1 N3 XX

	Тип	Відповідь	
1	X	-	
2	O	- HI	Т2. В связи с чем вас сегодня проверяют на полиграфе? В связи с домашним конфликтом
3	N1	- HI	В связи с конфликтом на дороге
4	N2	- HI	В связи с предстоящей командировкой
5	R1	- ТАК	Ее версия - в связи с утечкой информации с компании
6	N3	- HI	В связи с расширением бизнеса
7	XX	-	

Рис. 7.1. Тест правдивого «да» из диагностического блока опросника по МВСИ



Рис. 7.1.1 Полиграмма к тесту правдивого «да» из диагностического блока опросника по МВСИ

Тест 1 | Тест 2 | **Тест 3** | Тест 4 | Тест 5 | **Тест 6** | Тест 7 | Тест 8 | Тест 9 | Тест 10 |

v 1 | X O N1 R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 R11 R12 R13 XX

	Тип	Відповідь	
1	X	-	
2	O	- ТАК	Т4. Что вам АТВ об атаке на компанию? Вам АТВ, из какой системы были скачаны файлы
3	N1	- ТАК	Вам АТВ, какая информация о компании была раскрыта вследствие атаки
4	R1	- НІ	Вам АТВ, кто организовал эту атаку на компанию
5	R2	- НІ	Вам АТВ, какие планы у причастных к атаке
6	R3	- НІ	Вам АТВ, кто из действующих сотрудников причастен к атаке
7	R4	- НІ	Вам АТВ, кто конкретно стоит за атакой на компанию
8	R5	- НІ	Вам АТВ, какая конечная цель у причастных к атаке
9	R6	- НІ	Вам АТВ, кто из сотрудников имеет отношение к атаке на компанию
10	R7	- НІ	Вам АТВ, через какие мессенджеры общаются причастные к атаке
11	R8	- НІ	Вам АТВ, кто решал, какие именно файлы надо скачать с
12	R9	- НІ	Вам АТВ, по каким каналам связи участники атаки доводят друг другу инф-цию
13	R10	- НІ	Вам АТВ, кто сливал файлы на с ча внешние ресурсы
14	R11	- НІ	Вам АТВ, где именно встречаются причастные к атаке на компанию
15	R12	- НІ	Вам АТВ, кто загрузил старый файл с на сайт компании
16	R13	- ТАК	Ее версия или повтор макс пары
17	XX	-	

Рис. 7.2. Тест Татьяны Кузьмич «Что вам абсолютно точно известно об атаке на компанию?» из диагностического блока опросника по МВСИ

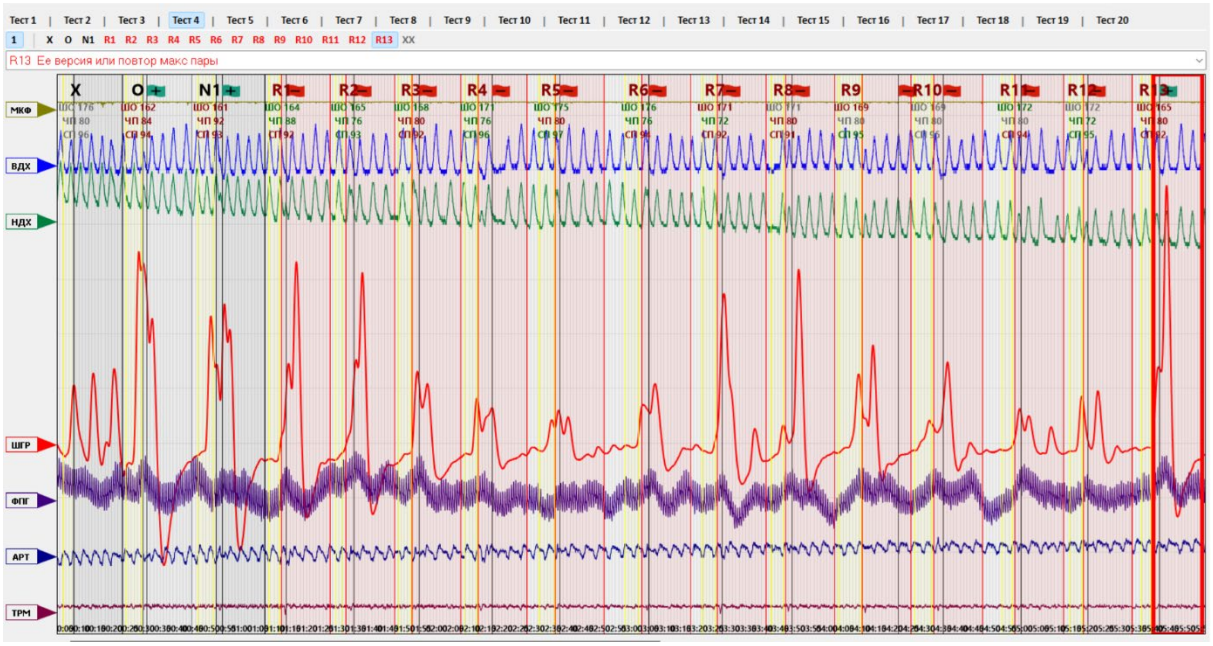
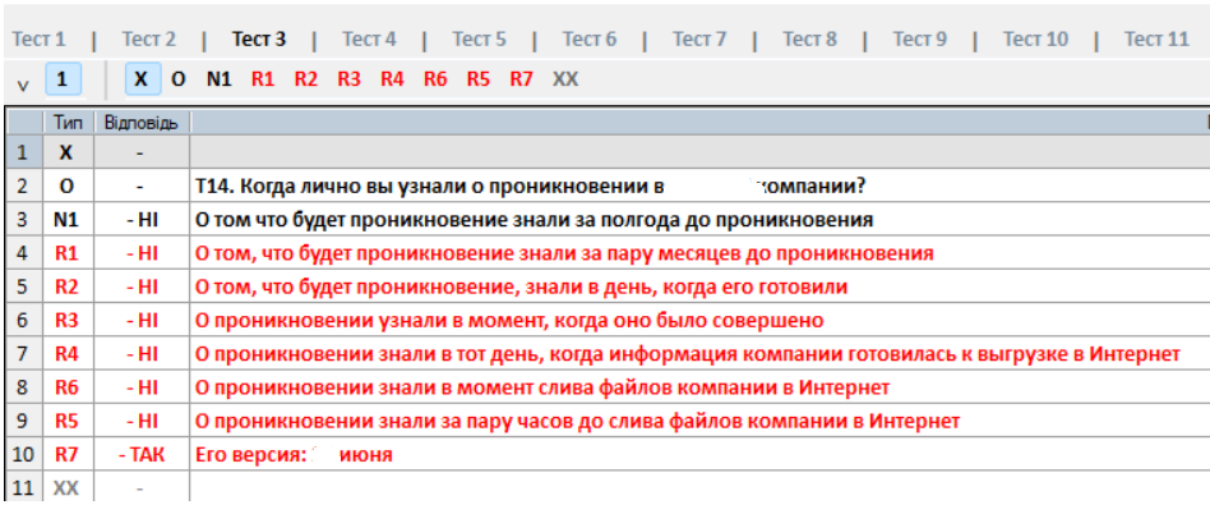


Рис. 7.2.1 Полиграмма к тесту Татьяны Кузьмич «Что вам абсолютно точно известно об атаке на компанию?» из диагностического блока опросника по МВСИ

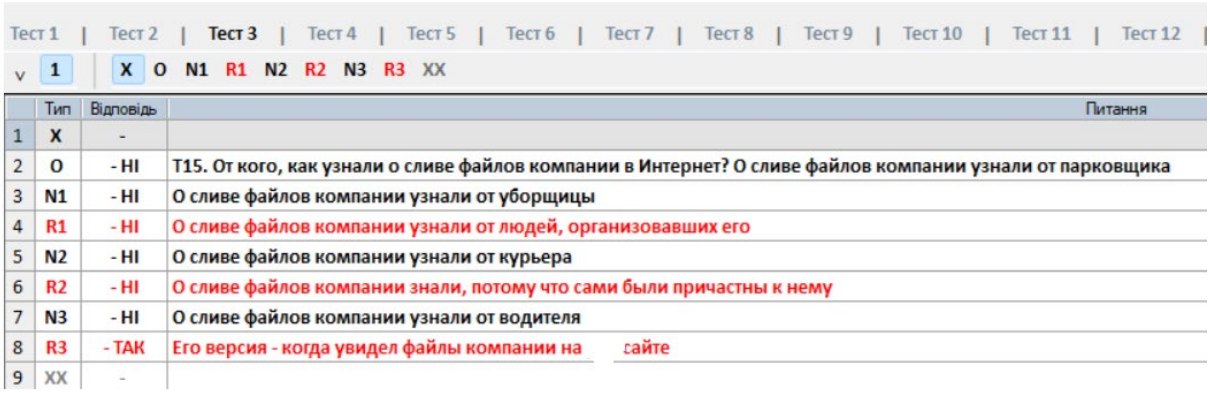


	Тип	Відповідь	
1	X	-	
2	O	-	Т14. Когда лично вы узнали о проникновении в омпании?
3	N1	- НІ	О том что будет проникновение знали за полгода до проникновения
4	R1	- НІ	О том, что будет проникновение знали за пару месяцев до проникновения
5	R2	- НІ	О том, что будет проникновение, знали в день, когда его готовили
6	R3	- НІ	О проникновении узнали в момент, когда оно было совершено
7	R4	- НІ	О проникновении знали в тот день, когда информация компании готовилась к выгрузке в Интернет
8	R6	- НІ	О проникновении знали в момент слива файлов компании в Интернет
9	R5	- НІ	О проникновении знали за пару часов до слива файлов компании в Интернет
10	R7	- ТАК	Его версия: июня
11	XX	-	

Рис. 7.3. Тест на время получения респондентом информации об атаке на компанию из четвертого блока опросника по МВСИ



Рис. 7.3.1 Полиграмма к тесту на время получения респондентом информации об атаке на компанию из четвертого блока опросника по МВСИ



	Тип	Відповідь	Питання
1	X	-	
2	O	- НІ	Т15. От кого, как узнали о сливе файлов компании в Интернет? О сливе файлов компании узнали от парковщика
3	N1	- НІ	О сливе файлов компании узнали от уборщицы
4	R1	- НІ	О сливе файлов компании узнали от людей, организовавших его
5	N2	- НІ	О сливе файлов компании узнали от курьера
6	R2	- НІ	О сливе файлов компании знали, потому что сами были причастны к нему
7	N3	- НІ	О сливе файлов компании узнали от водителя
8	R3	- ТАК	Его версия - когда увидел файлы компании на сайте
9	XX	-	

Рис. 7.4 Тест на источник осведомленности респондента об атаке на компанию из четвертого блоку опросника по МВСИ



Рис. 7.4.1 Полиграма к тесту Тест на источник осведомленности респондента об атаке на компанию из четвертого блоку опросника по МВСИ

Таким образом, анализ результатов проведенных исследований позволяет прийти к следующим выводам:

1. Технологический прогресс не только не устранил человека как источник потенциальной угрозы для информационной безопасности, но и, напротив, привел к масштабированию возможных последствий его сознательных противоправных действий либо мотивированного или немотивированного бездействия, халатности.

2. Полиграфология имеет значительные перспективы дальнейшего развития и применения при предупреждении и расследовании случаев несанкционированного проникновения в электронную систему компании.

3. Особенно эффективной полиграфология является в том случае, когда полиграфолог на профессиональном уровне владеет методикой выявления Скрываемой информации и способен провести полноценный кадровый аудит, а не ограничиваться выводом о причастности/непричастности конкретного сотрудника к проникновению в электронную систему компании.

Использованные источники:

1. Криміналістика : підручник / [В. М. Шевчук, В. А. Журавель, В. Ю. Шепітько та ін.]; за ред. В. М. Шевчука : Нац. юрид. ун-т ім. Ярослава Мудрого. – Харків : Право, 2024. С. 488–510.

2. Морозова Т. Р. Поліграфологія: підручник / за ред. О. М. Морозова. Харків: «Естет Принт», 2019. 478 с.

3. Морозова Т. Р. Методика виявлення прихованої інформації у поліграфологічних

дослідженнях : монографія. Вид. 2-ге, доповн. і переробл. / за наук. ред. О. М. Морозова. Київ : Алерта, 2026. С. 189–202.