Морозова Тетяна Романівна,
доктор психологічних наук, професор,
атестований судовий експерт,
президент Всеукраїнської асоціації поліграфологів

Методика виявлення прихованої інформації: розслідування несанкціонованого проникнення в електронну систему компанії

Вже десятки років бізнес, незалежно від його розміру та рівня технологічності, неможливо уявити без використання програмного забезпечення як загальнопоширеного, так і розробленого спеціально під потреби та на замовлення конкретної компанії. Однак розвиток технологій не дав бізнесменам бажаного інформаційного захисту, радше навпаки: та фінансова інформація, яку раніше доводилося збирати по крихтах, із залученням агентурного апарату та ризиком його викриття, зараз може бути викрадена за один-декілька несанкціонованих входів завдяки менеджеру середньої ланки, який елементарно не налаштував двофакторну автентифікацію. Ті суми, які раніше злодій викрадав фізично із сейфа, ризикуючи бути виявленим на місці вчинення злочину, зафіксованим на камерах відеоспостереження, частіше нікчемні у порівнянні із грошима, що виводить хакер електронним способом, перебуваючи при цьому за тисячі кілометрів від жертви злочину. Ті масиви компромату на компанію, для отримання яких колись потрібно було залучати групу приватних детективів/розслідувачів, чия активність не могла залишатися довго непомітною, зараз можуть бути скачані протягом однієї ночі, але при цьому завдати бізнесу нищівного удару, зробити його заручником вимагачів і шантажистів [1].

Поза тим, є речі, які залишаються незмінними:

- злочини планують і реалізують конкретні люди;
- для реалізації злочинного задуму необхідно як мінімум скористатися вразливістю електронної системи, яка може бути в тому числі майстерно замаскована під банальну халатність конкретного працівника;
- співробітники, нелояльні до компанії, ті, хто не розділяє її цінності та не відчуває внутрішньої залученості до команди і справи, апріорі схильні до саботажу інструктажів щодо інформаційної безпеки, їхня бездіяльність є не менш небезпечною, аніж сплановані шкідницькі дії;
- фаворитизм, підбір фахівців, які відповідають за кібербезпеку за принципом особистої зручності для керівників середньої ланки, а не на підставі професійності, рано чи пізно закінчується для компанії втратою даних, грошей або й репутації.

Аналіз 41 поліграфологічного дослідження, проведеного у 2025–2026 рр. за допомогою методики виявлення прихованої інформації (МВПІ) у рамках службових розслідувань за фактами несанкціонованого проникнення у внутрішні системи трьох різних компаній, дозволив визначити обов’язкові складові тестових опитувальників,

розроблених для таких випадків. Безумовно, кожна ситуація мала свої відмінності, зокрема відрізнялися способи обходу існуючих у компаніях систем захисту інформації та кінцеві наслідки інцидентів: в одних випадках це було викладення компрометуючої інформації на зовнішні ресурси, в інших – виведення коштів і т. д. Однак було й багато спільного у перебігу надзвичайної події, а стосовно замовників – то вони були практично одностайні як у своїх підозрах і занепокоєннях, так і у змісті питань, винесених спеціалісту на вирішення.

Узагальнення результатів успішно проведених тестувань, що, окрім іншого, згодом отримали підтвердження з боку незалежного технічного аудиту, показує, що в третьому блоці таких опитувальників повинні бути передбачені питання, які дозволяють встановити у респондента наступне:

1) інформованість респондента щодо осіб, причетних до атаки на компанію.

Із цією метою можуть бути використані тести перевірки версій на кшталт «Чи відомо вам, що насправді відбувається?», «Чи відомо вам, хто насправді атакує компанію?», «Що із переліченого стосується вас особисто?», із оформленням просоціальної версії респондента у питаннях: «Компанію атакувала група невідомих вам особисто людей?», «Компанію атакувала група людей, про яких ви нічого не знаєте?», «Ви дійсно не знаєте, хто атакував компанію?» [2, 3].

Приклади тестів і поліграм до них наведені нижче у 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 |

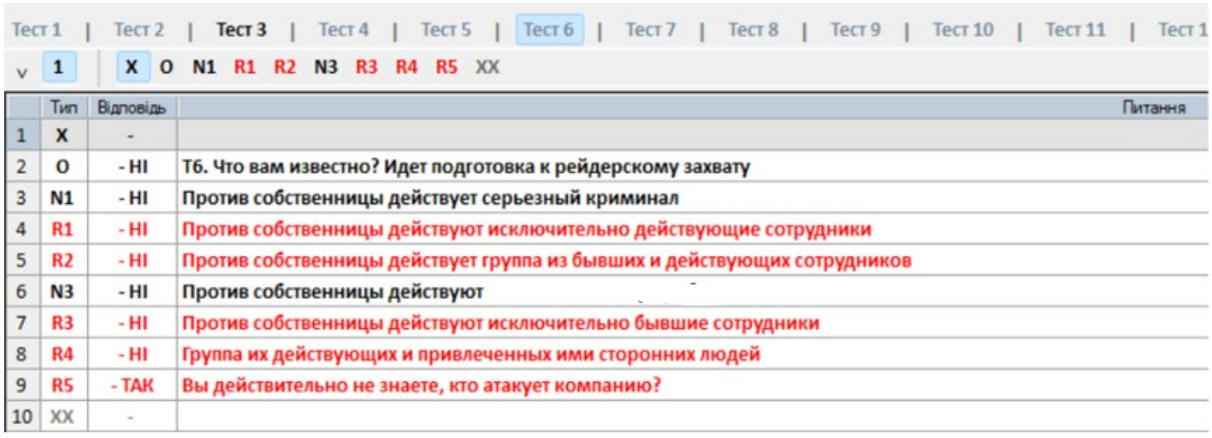
v **1** **X** **O** **N1** **R1** **R2** **N3** **R3** **R4** **R5** **XX**

	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

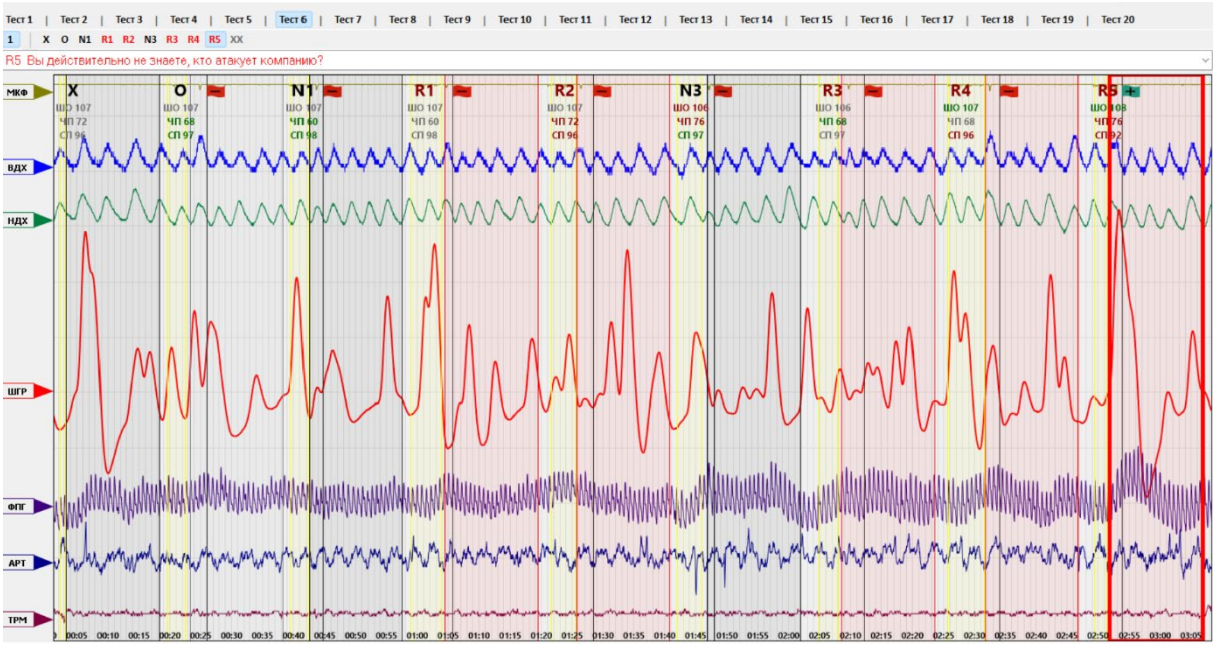
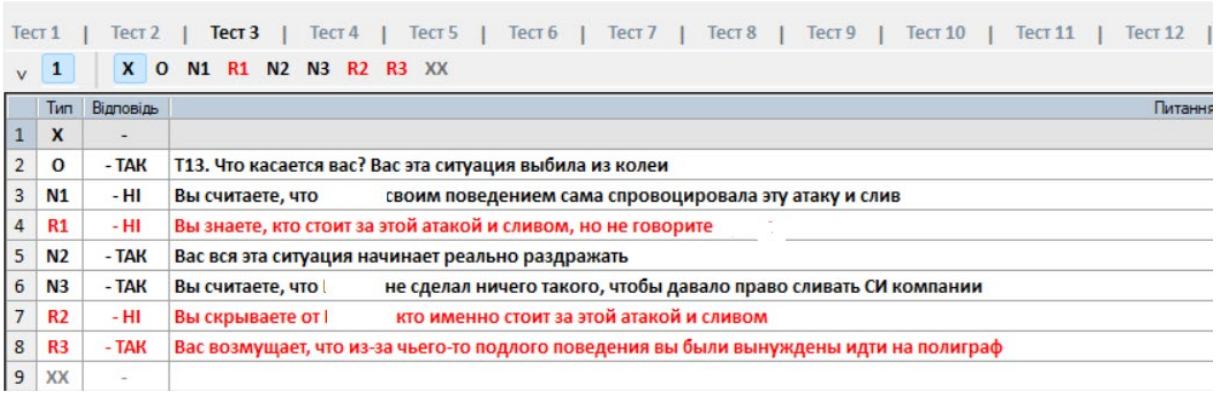


Рис. 1.2.1



	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

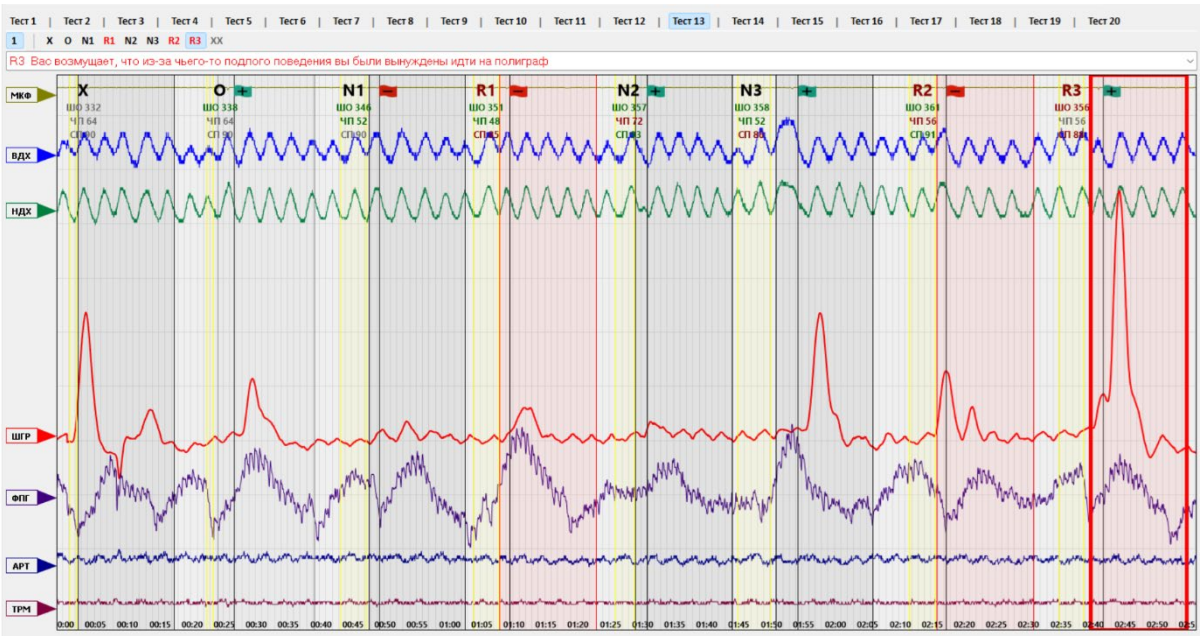


Рис. 1.3.1

2) лояльність/нелояльність респонедента по відношенню до компанії, керівництва: байдужість, внутрішня підтримка атаки, сприйняття її як допустимого способу зведення рахунків із керівництвом, або засудження атаки, переживання за можливі негативні наслідки для компанії.

Із цією метою можуть бути використані тести перевірки версій на кшталт «Хто ви, реально, у ситуації атаки на компанію?», «Ваше відношення до атаки на компанію?» із питаннями-версіями респондентів, які вони озвучать у передтестовій, посередтестових бесідах.

Приклади тестів і поліграм до них наведені нижче у 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

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

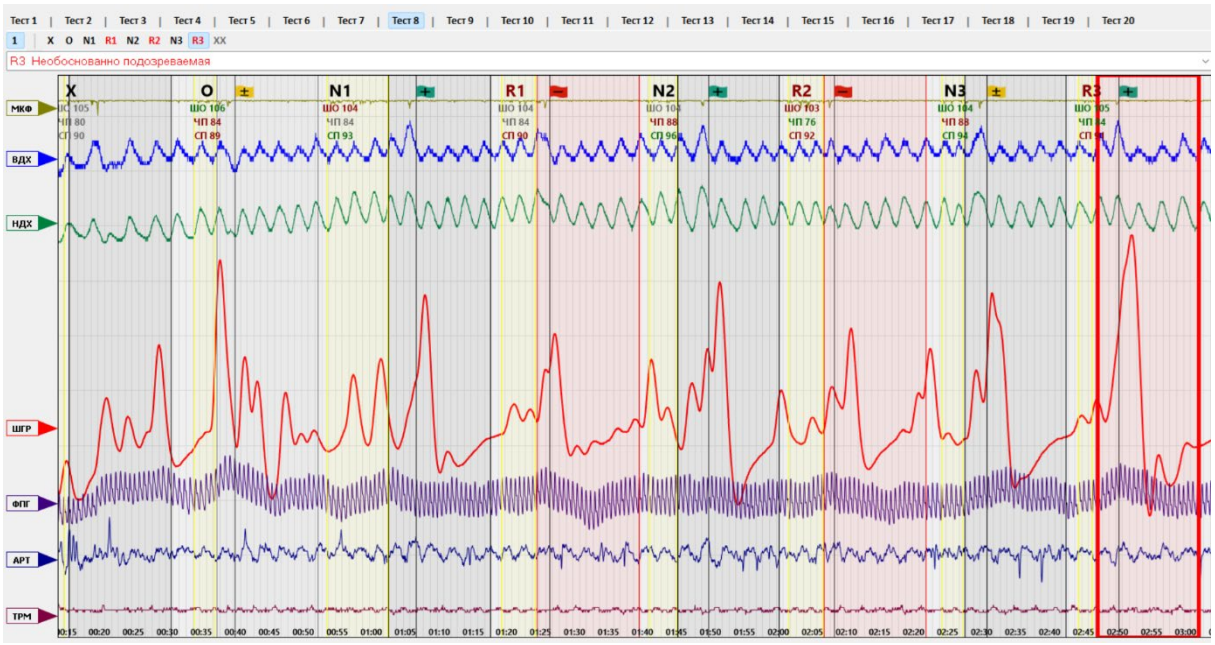
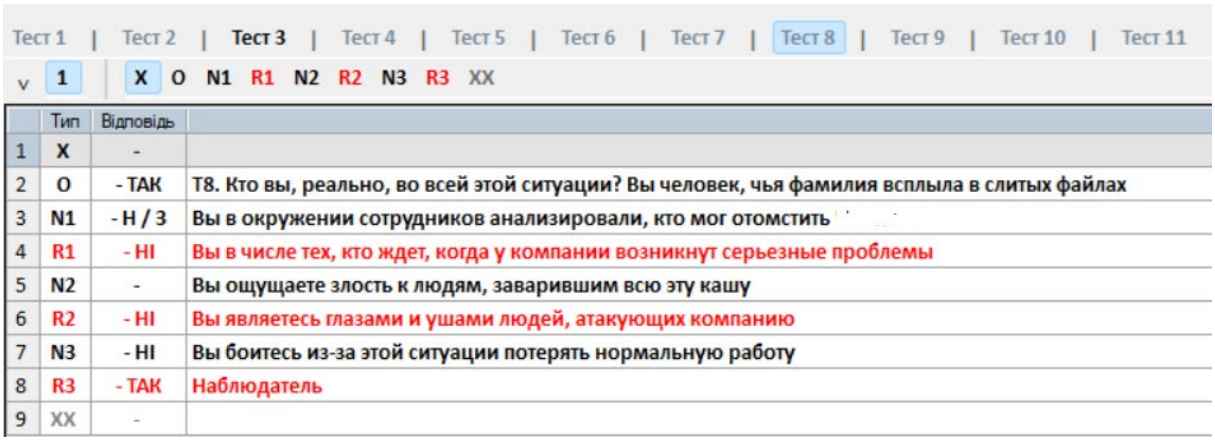


Рис. 2.1.1

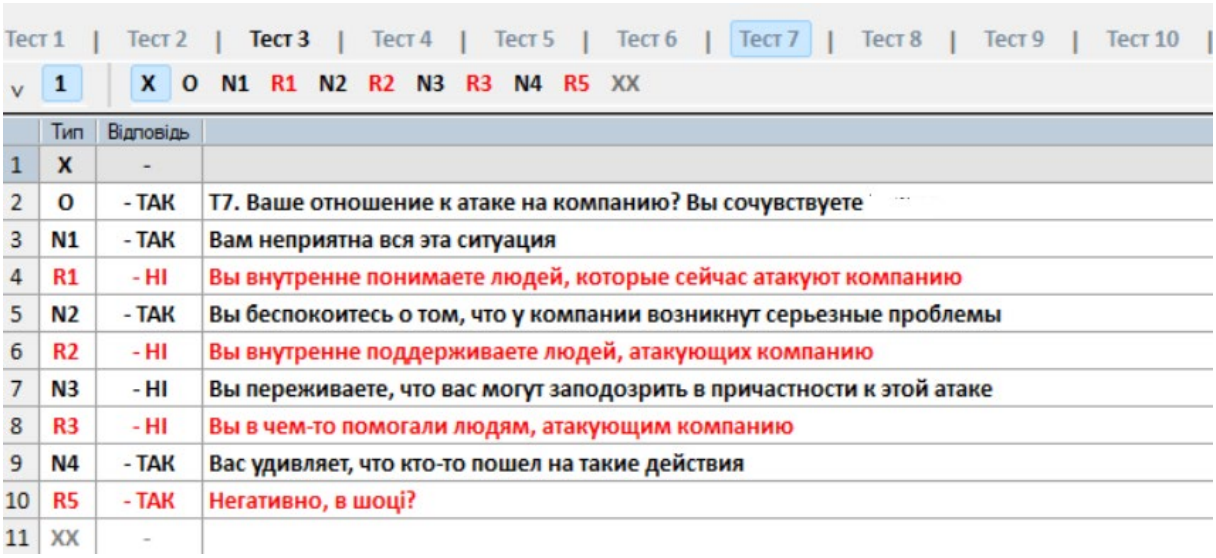


	Тип	Відповідь	
1	X	-	
2	O	- ТАК	Т8. Кто вы, реально, во всей этой ситуации? Вы человек, чья фамилия всплыла в слитых файлах
3	N1	- Н / З	Вы в окружении сотрудников анализировали, кто мог отомстить
4	R1	- НІ	Вы в числе тех, кто ждет, когда у компании возникнут серьезные проблемы
5	N2	-	Вы ощущаете злость 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

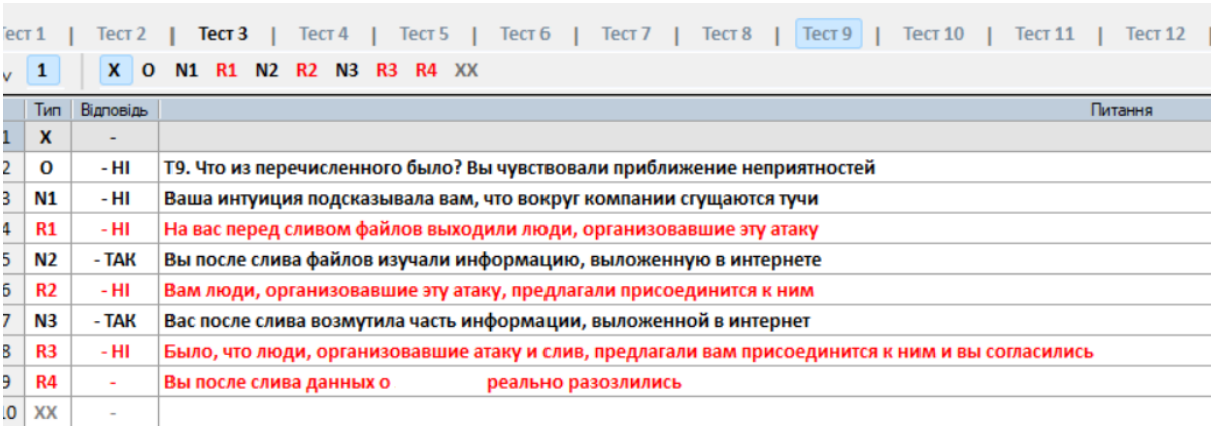


Рис. 2.3.1

3) залученість респондента-співробітника компанії організаторами атаки до її здійснення.

Із цією метою можуть бути використані тести на знання невідомого рішення на кшталт «Що із перерахованого відбувалося особисто з вами?», якими з'ясовується, чи контактували причетні до атаки із респондентом, чи пропонували долучитися до них, чи прийняв він цю пропозицію; чи брав він участь у плануванні та обговоренні атаки? [2, 3].

Приклади тестів і поліграм до них наведені нижче у рис. 3.1–3.2.1;

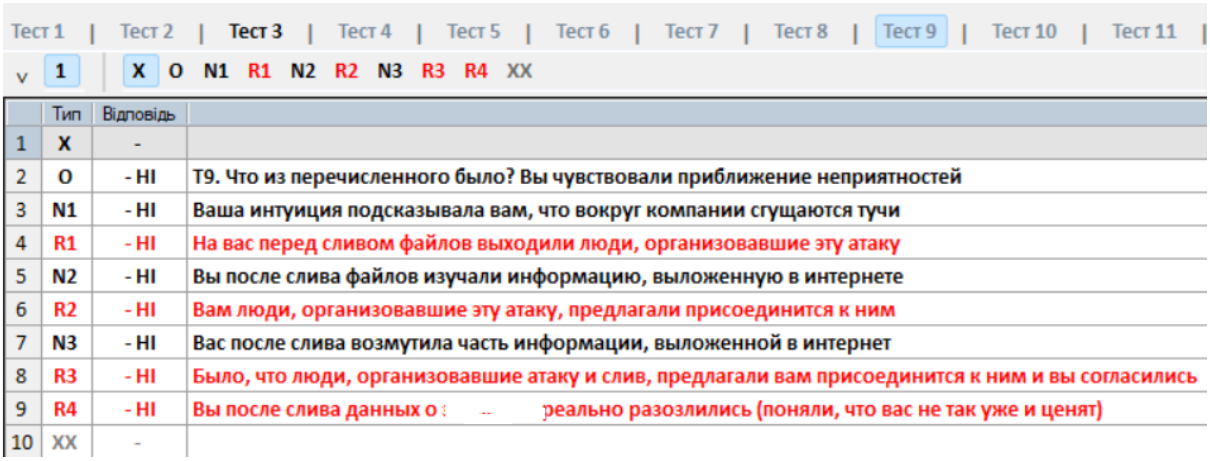


	Тип	Відповідь	Питання
1	X	-	
2	O	- НІ	Т9. Что из перечисленного было? Вы чувствовали приближение неприятностей
3	N1	- НІ	Ваша интуиция подсказывала вам, что вокруг компании сгущаются тучи
4	R1	- НІ	На вас перед сливом файлов выходили люди, организовавшие эту атаку
5	N2	- ТАК	Вы после слива файлов изучали 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) ініціювання респондентом-співробітником компанії атаки та залучення до неї інших.

Із цією метою можуть бути використані тести на знання невідомого рішення на кшталт «Що із перерахованого відбулося особисто із вами?», якими з'ясовується, чи виходив на когось респондент із пропозицією взяти участь у атаці, чи отримував він від когось згоду щодо участі у ній; чи планував, обговорював атаку на етапі її підготовки?

Приклади тестів і поліграм до них наведені нижче у 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

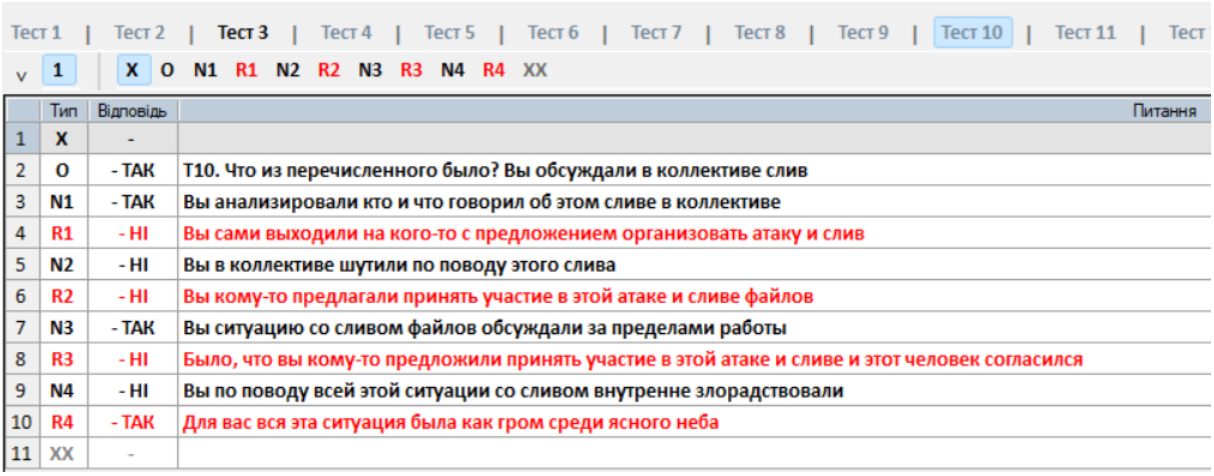
v 1 | X O N1 R1 N2 R2 N3 R3 N4 R4 N5 R5 XX

	Тип	Відповідь	Питання
1	X	-	
2	O	- ТАК	Т11. 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) наявність у респондента-співробітника компанії комунікації зі зловмисниками після атаки.

Із цією метою можуть бути використані тести на знання невідомого рішення на кшталт «Що із переліченого мало місце?», якими з'ясовується, чи контактував респондент із причетними до атаки після її вчинення, чи розповідав їм, якого психологічного ефекту вони досягли, які настрої у компанії, як поводиться і що говорять з приводу атаки керівники та співробітники?

Приклади тестів і поліграм до них наведені нижче у 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	- HI	T12. Какие факты имели место? У вас на этой работе были конфликты
3	N1	- HI	Вы на этой работе конфликтовали с другими сотрудниками
4	R1	- HI	О настроениях в компании после слива рассказывали врагам компании
5	N2	- HI	Вы на этой работе конфликтовали с руководством
6	R2	- HI	Говорили причастным к атаке, что после слива говорили конкретные сотрудники
7	N3	- HI	Вы на этой работе на других сотрудников перекидывали свою вину
8	R3	- HI	Передавали причастным к атаке, что после слива говорила
9	N4	- HI	Вас на этой работе кто-то подставлял
10	R4	- HI	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

б) свідоме ігнорування, невиконання респондентом правил інформаційної безпеки.

Логічно, що спочатку потрібно з’ясувати за допомогою окремого тесту, чи проводився із респондентом відповідний інструктаж, які саме із доведених застережень/заборон він порушив, а лише потім – чому, на його думку, стала можливою ця атака.

Приклади тестів і поліграм до них наведені нижче у 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 |

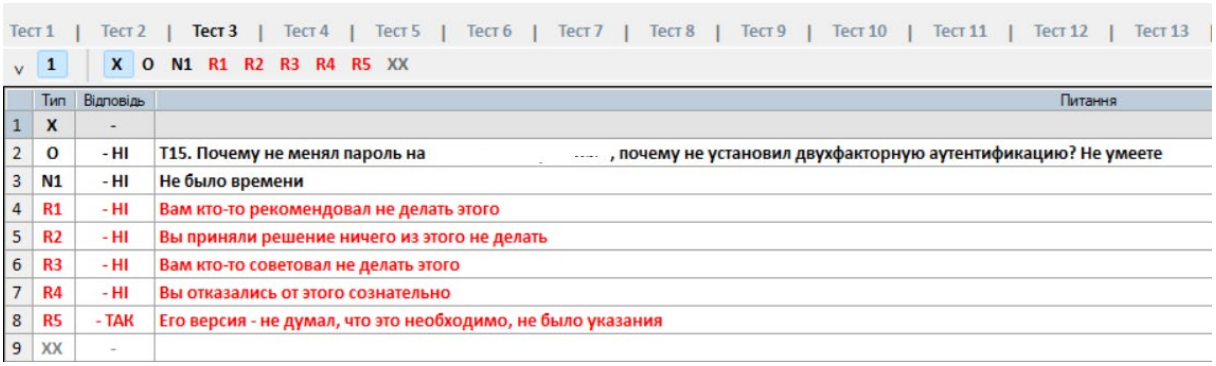
v 1 | X O N1 R1 R2 R3 R4 R5 XX

	Тип	Відповідь	Питання
1	X	-	
2	O	- НІ	Т13. Что из перечисленного было? Вы забывал пароль входа в систему
3	N1	- НІ	Вы сами заражали свой служебный ПК вирусами
4	R1	- НІ	Вам на работе доводили сведения о потенциальных уязвимостях
5	R2	- НІ	Вам на работе доводили требования информационной безопасности
6	R3	- НІ	Вы на работе доводили принятые в компании процедуры предупреждения хакерских атак
7	R4	- НІ	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

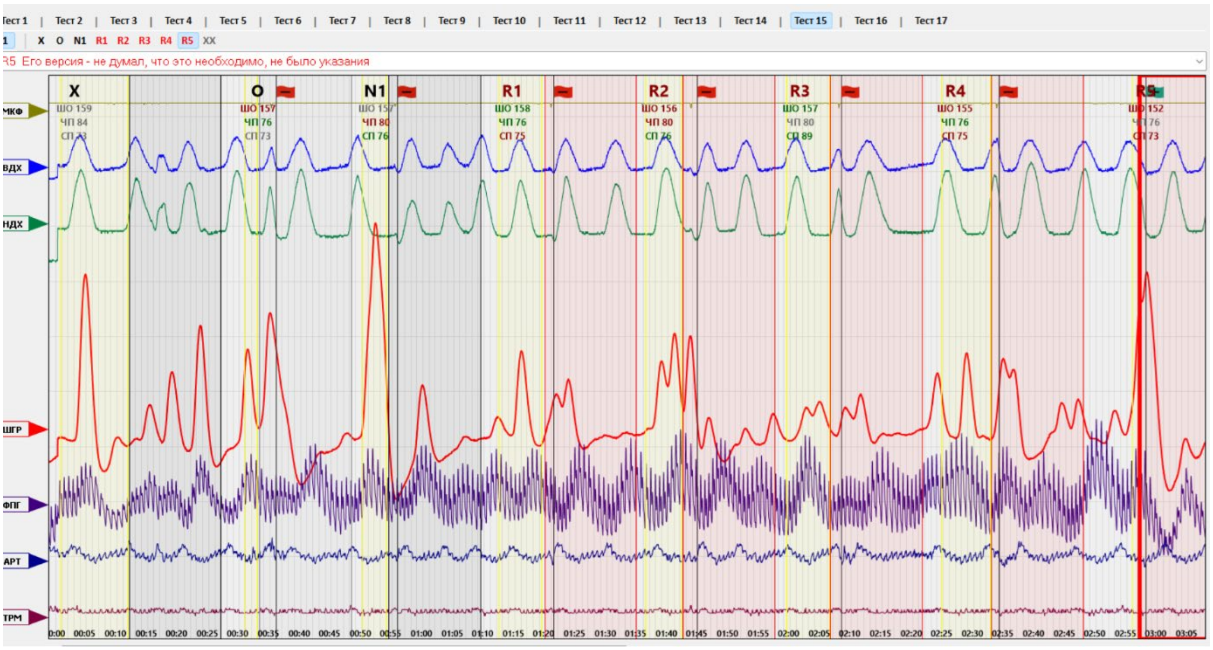


Рис. 6.2.1

Що стосується стимульного, діагностичного (тест Тетяни Кузьмич «Що вам абсолютно точно відомо про атаку на компанію?») та четвертого блоку тестових опитувальників, призначених для використання з метою розслідування несанкціонованого проникнення в електронну систему компанії – то вони є традиційними для МВПІ, а правила їхнього формулювання детально описані у підручнику та монографії [2, 3].

Вказані тести та одержані за їх допомогою поліграми наведені у 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 |

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

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

Рис. 7.1. Тест правдивого «так» із діагностичного блоку опитувальника за МВПІ



Рис. 7.1.1 Поліграма до тесту правдивого «так» із діагностичного блоку опитувальника за МВПІ

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 Тетяни Кузьмич «Що вам абсолютно точно відомо про атаку на компанію?» із діагностичного блоку опитувальника за МВПІ

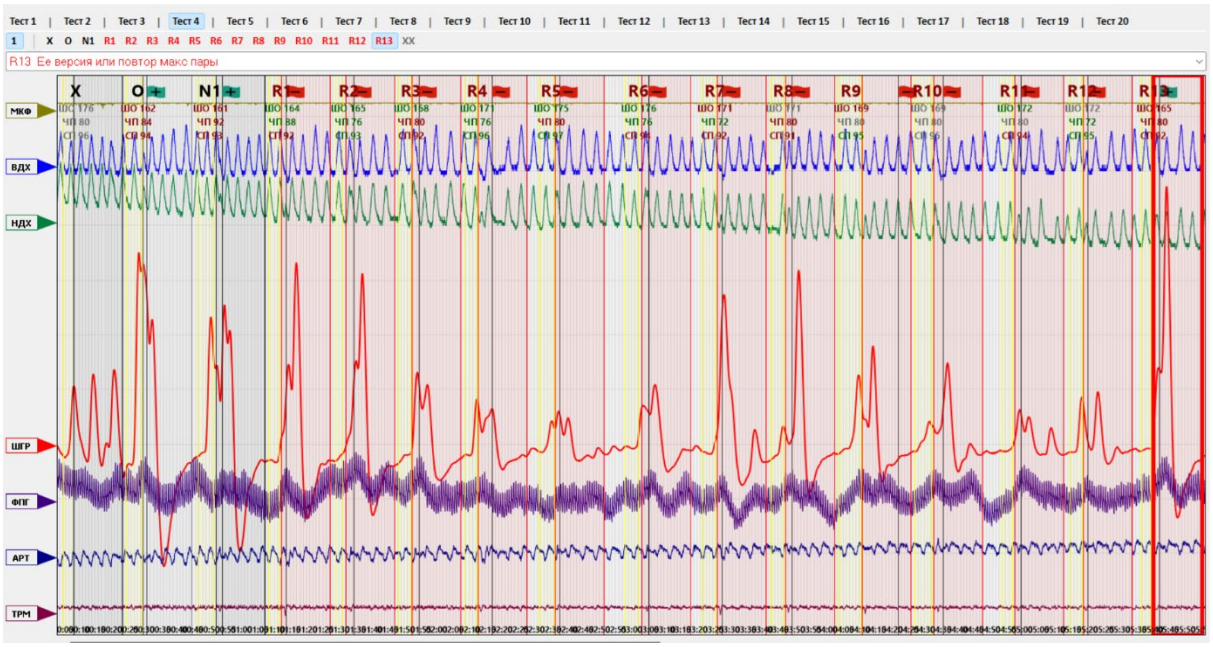


Рис. 7.2.1 Поліграма до тесту Тетяни Кузьмич «Що вам абсолютно точно відомо про атаку на компанію?» із діагностичного блоку опитувальника за МВПІ

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 R2 R3 R4 R6 R5 R7 XX

	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 час отримання респондентом інформації про атаку на компанію із четвертого блоку опитувальника за МВПІ



Рис. 7.3.1 Поліграма до тесту на час отримання респондентом інформації про атаку на компанію із четвертого блоку опитувальника за МВПІ

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 | XX

	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 джерело обізнаності респондента про атаку на компанію із четвертого блоку опитувальника за МВПІ



Рис. 7.4.1 Поліграма до тесту на джерело обізнаності респондента про атаку на компанію із четвертого блоку опитувальника за МВПІ

Таким чином, аналіз результатів проведених досліджень дозволяє дійти наступних висновків:

1. Технологічний прогрес не лише не усунув людину як джерело потенційної загрози для інформаційної безпеки, навпаки, він призвів до масштабування можливих наслідків її свідомих протиправних дій або мотивованої чи немотивованої бездіяльності, халатності.
2. Поліграфологія має значні перспективи подальшого розвитку і застосування при попередженні та розслідуванні випадків несанкціонованого проникнення в електронну систему компанії.
3. Особливо ефективною поліграфологія є у тому випадку, коли поліграфолог на професійному рівні володіє методикою виявлення прихованої інформації та здатний провести повноцінний кадровий аудит, а не обмежитися висновком щодо причетності/непричетності конкретного співробітника до проникнення в електронну систему компанії.

Використані джерела:

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.