СОЦИОЛОГИЯ РИСКА

DOI: 10.19181/socjour.2021.27.4.8649

К.А. ГАВРИЛОВ[1,2], М.В. БУТЫНКО[3]

[1] Национальный исследовательский университет
«Высшая школа экономики».
101000, Москва, ул. Мясницкая, д. 20.
[2] Институт социологии ФНИСЦ РАН.
109544, Москва, ул. Большая Андроньевская, д. 5, стр. 1.
[3] Государственное казенное учреждение города Москвы
«Информационный город».
105064, Москва, Нижний Сусальный пер., д. 5, стр. 16.

ВОСПРИЯТИЕ ТРАДИЦИОННЫХ РИСКОВ И КИБЕРРИСКОВ: ОПЫТ ИСПОЛЬЗОВАНИЯ «ПСИХОМЕТРИЧЕСКОЙ ПАРАДИГМЫ»[1]

Аннотация. В статье приводится опыт использования «психометрической парадигмы» (П. Словик, С. Лихтенштейн, Б. Фишхоф и др.) для изучения восприятия киберрисков и сравнения их с другими рисками, обозначенными как «традиционные». Респондентам в ходе онлайн-опроса предъявлялось 7 киберрисков (от компьютерных игр до хакерских атак и вирусов) и 65 традиционных рисков (от природных катастроф до атомных электростанций и терроризма), оцениваемых по 8 характеристикам. В результате выявлено, что компьютерные игры воспринимаются иначе по сравнению с остальными киберрисками: прежде всего они не вызывают страха. Остальные кибериски локализованы в области скорее неизвестных и умеренно страшных рисков, не образуя при этом отдельный кластер. Ближе всего к киберрискам в двумерном пространстве восприятия риска оказались радиационная терапия, гербициды и пестициды. Результаты проведенного поискового исследования могут быть рассмотрены как отражение использованной выборки, где основными участниками оказались активные интернет-пользователи, способные делать различия между предъявляемыми киберрисками.

Ключевые слова: кибериски; риск; восприятие риска; психометрическая парадигма.

---

[1] Публикация подготовлена в ходе проведения исследования (№ 20-01-023) в рамках Программы «Научный фонд Национального исследовательского университета “Высшая школа экономики” (НИУ ВШЭ)» в 2020–2021 гг.

Авторы признательны двум анонимным рецензентам «Социологического журнала», чьи замечания и пожелания позволили улучшить качество статьи.

Для цитирования: *Гаврилов К.А., Бутынко М.В.* Восприятие традиционных рисков и киберрисков: опыт использования «психометрической парадигмы» // Социологический журнал. 2021. Том 27. № 4. С. 146–168. DOI: 10.19181/socjour.2021.27.4.8649

Постановка исследовательской задачи

Тематика киберрисков, или рисков информационной безопасности, привлекает все большее внимание как в дискурсе массмедиа, так и в научных исследованиях. Имеется немало работ, посвященных киберрискам и информационной безопасности в социальных науках, в том числе их общетеоретическому осмыслению [27]. Отдельным направлением становится изучение особенностей восприятия киберрисков [14; 16; 17; 20; 21; 28; 29]. В центре внимания этих работ — вопрос о том, каким образом киберриски воспринимаются не экспертами по информационным технологиям [30], не представителями компаний [15], а неспециалистами — как населением в целом, так и отдельными группами, например, подростками [21]. Однако в рамках данного направления не предпринимается попытка сравнить восприятие киберрисков с «традиционными» рисками, в результате чего остается неясным, например, на какие риски в общественном восприятии похожи киберриски, являются ли различия между киберрисками несущественными на фоне разницы с другими рисками.

Эти вопросы оказались в центре внимания нашего исследования. Мы предприняли попытку изучить особенности восприятия киберрисков с помощью методики «психометрической парадигмы», предложенной П. Словиком и его коллегами (С. Лихтенштейн, Б. Фишхофом и др.) в 1970–1980-е гг. [24; 25]. Методология «психометрической парадигмы» позволяет выявить факторы, определяющие пространство восприятия риска. Соответственно, мы хотели определить положение киберрисков в этом пространстве и соотнести его с «традиционными» рисками. Сразу отметим, что в данной работе под «традиционными» рисками понимаются те, что ранее фигурировали у авторов «психометрической парадигмы» (и в этом смысле среди них имеются сравнительно новые риски, например, атомные электростанции или ВИЧ/СПИД), то есть речь может идти о вполне современных рисках.

Задачи нашего исследования имеют поисковый характер. Мы попытаемся, во-первых, выявить особенности восприятия киберрисков и, во-вторых, соотнести киберриски с «традиционными» рисками с помощью инструментария «психометрической парадигмы». Как будет показано далее, использование невероятностной выборки не позволит распространить полученные результаты на какую-либо совокупность (например, на население нашей страны или на пользователей Интернета), так что результаты по первой задаче будут иметь предварительный характер и позволят сформулировать гипотезы для будущих исследований. Эта же оговорка справедлива и для второй задачи; впрочем, мы надеемся, что выявленные паттерны будут не только отражать специфику нашей выборки, но и иметь более универсальный характер.

Имеющиеся исследования восприятия киберрисков в большей степени ориентированы на изучение различий между киберрисками [14; 16;

28; 29] и поэтому не позволяют выдвинуть гипотезы о месте этих рисков в пространстве восприятия. Можно лишь осторожно предположить, что эти риски будут восприниматься как сравнительно неизвестные, что они едва ли будут вызывать значительный страх. Что касается соотнесения с «традиционными» рисками, мы исходим из гипотезы, что киберриски в пространстве восприятия рисков — в силу своей схожей природы — будут занимать более близкие позиции друг к другу, чем по отношению к другим рискам. Эмпирически это может означать, что в контексте измерений восприятия риска киберриски образуют отдельный кластер, не пересекающийся с другими рисками. Альтернативная гипотеза, основанная на предшествующих работах, показавших существенные различия между киберрисками [28; 29], заключается в том, что киберриски будут рассредоточены в пространстве восприятия риска, и, как следствие, отдельные киберриски окажутся близки некоторым «традиционным» рискам.

«Психометрическая парадигма» в исследовании риска и киберриски

Основная задача представителей «психометрической парадигмы» — выявление факторов, влияющих на восприятие риска населением [24; 25]. Процедура эмпирического исследования в рамках данного подхода обычно включает следующие шаги.

1. Формируется перечень рисков, охватывающих либо разные, либо одну содержательную область (например, «социетальные» [8] или технологические риски [13]). Обычно этот перечень состоит из нескольких десятков единиц.

2. Принимается решение о перечне используемых суждений, по которым будут оцениваться все риски. Большинство таких суждений — это характеристики, которые могут быть потенциально применимы ко всем рискам. Перечень суждений варьируется от исследования к исследованию (один из наиболее полных представлен в таблице 1), но практически никогда их не меньше 8–9.

3. Участникам исследования предлагается оценить каждый риск по всем суждениям. Иными словами, предлагается весьма «затратная» для респондента процедура: при 30 рисках и 8 суждениях каждому участнику нужно сделать 240 оценок.

4. Полученные результаты чаще всего усредняются по респондентам, то есть из матриц с оценками респондентом каждого риска конструируется агрегированная матрица вида «риски – характеристики».

5. Для анализа агрегированной матрицы обычно используется факторный анализ методом главных компонент. В результате его применения выявляются специфические факторы восприятия риска. Как правило, речь шла о двух факторах:

– «неизвестность» / «незнание риска» (следствие непосредственной ненаблюдаемости риска, отложенности, новизны и др.);

– «страх перед риском» (связан с воспринимаемой неспособностью контролировать риск, катастрофическими последствиями, недобровольностью и последствиями для будущих поколений) [24, p. 281].

Изучаемые риски размещаются в этом двумерном пространстве, что позволяет судить о «похожести» разных типов рисков.

Таблица 1

Характеристики риска, использованные представителями «психометрической парадигмы»

№ п/п	Суждения	Описание (задаваемый вопрос)
1	***Недобровольность риска***	Добровольно или нет попадают люди в эти рискованные ситуации?
2	***Отложенность воздействия***	Насколько быстро наступает смерть в результате воздействия этого риска. Смерть наступит немедленно или позже?
3	***Неизвестность людям***	Насколько хорошо или плохо информированы о данном риске люди, которые ему подвергаются?
4	***Неизвестность науке***	Насколько хорошо или плохо этот риск известен науке?
5	***Неконтролируемость***	Если Вы подвержены данному риску, то можете ли Вы или не можете посредством личных навыков или усердия избежать смерти от воздействия этого риска?
6	***Новизна***	Являются ли такие риски новыми, неизвестными ранее, или они стары, хорошо знакомы?
7	***Катастрофичность***	Убивает ли такой риск людей постепенно (хронический риск) или сразу убивает большое число людей (катастрофический риск)?
8	***Страх***	Является ли риск таким, что люди научились жить с ним и думать о нем достаточно спокойно, или он в значительной степени страшен для них – на уровне инстинкта?
9	*Смертельность последствий*	Когда этот риск имеет место, насколько вероятно то, что его последствия будут смертельны?
10	Отсутствие превентивного контроля	Можно или нельзя предотвратить все риски такого рода?
11	Невозможность снижения риска	Если несчастье произошло, то можно ли уменьшить (контролировать) ущерб?
12	Угроза будущим поколениям	Угрожает ли риск будущим поколениям?
13	Опосредованность	Подвергается опасности прямо или опосредованно?
14	Справедливость рисков и выгод	Распределяются ли выгоды справедливо среди тех, кто подвержен риску?
15	Глобальный катастрофизм	Угрожает ли опасность глобальной катастрофой?
16	Динамика уровня риска	Риск увеличивается или уменьшается?

Примечание: Полужирным шрифтом выделены изученные нами характеристики, курсивом — характеристики исходного исследования 1978 г. [12].
Источник: [25, p. 86–86, 138] (с изменениями).

В наши задачи не входит более подробное описание методики «психометрической парадигмы» и результатов ее применения (об этом см. работы: [2; 11]). Отметим лишь несколько моментов.

Во-первых, несмотря на то что методика была предложена еще в конце 1970-х гг., она по-прежнему активно используется зарубежными исследователями, а двухфакторная структура восприятия риска, будучи ключевым эмпирическим результатом, неизменно воспроизводится, даже при попытке добавить новые измерения восприятия риска (см., например: [8]). Этому не помешала критика данного подхода, которая главным образом сосредоточена на шаге 4 описанной процедуры, то есть на процедуре агрегирования. Эта процедура приводит к потере индивидуальных различий в оценках, а выводы, полученные на агрегированной матрице, не соответствуют результатам анализа «индивидуальных матриц» [19]. Как результат в настоящее время попытки учесть эту критику (см., например: [10; 23]) сосуществуют с исследованиями, не затрагивающими проблему агрегирования [13].

Во-вторых, «психометрическая парадигма» эволюционирует в разных направлениях. Одним из таких направлений, как отмечают Б. Шовин и Д. Херман в своем обзоре [11], является включение новых тематик, областей изучаемых рисков. Применительно к нашему исследованию целесообразно остановиться на попытках изучить киберриски при помощи описываемой методики. Так, Хуанг с коллегами включили в свою методику ряд суждений «психометрической парадигмы» (тяжесть последствий, добровольность, катастрофичность и др.) для изучения 21 киберриска. Была выявлена шестифакторная структура восприятия риска, одним из ключевых оказался фактор «знание», что соответствует традиционно получаемым с помощью «психометрической парадигмы» результатам [16].

В. Гарг и Д. Кэмп изучали восприятие 15 киберрисков (от утечки персональных данных до спама и вирусов) при помощи 9 суждений из «психометрической парадигмы». В результате только 13% вариации объяснялось этими суждениями, сильнее всего дифференцировало риски суждение «тяжесть последствий». Также выяснилось, что значительную роль играет временной фактор: чем старее риски, тем меньше беспокойства они вызывают [14].

Ван Шаик с соавторами в нескольких работах [28; 29] использовали эти же 9 суждений для оценки 18 киберрисков. В частности, они выяснили, что опрошенные больше всего опасались рисков, связанных с утечкой персональных данных, кейлоггеров, кибербуллинга и социальной инженерии. Что касается факторов восприятия риска, то ключевыми предикторами оказались суждения «добровольность», «отложенность воздействия», «катастрофичность», «страх», «тяжесть последствий» и «неконтролируемость».

Таким образом, данные исследования показывают, что суждения из «психометрической парадигмы» позволяют дифференцировать ки-

берриски. При этом за пределами рассмотрения остается вопрос, как киберриски соотносятся с «традиционными» рисками. В частности, являются ли различия между киберрисками столь значительными, что они оказываются похожими на другие типы рисков, или, напротив, киберриски образуют отдельный кластер рисков, не пересекающихся с другими рисками? Не менее интересно и то, какое место киберриски занимают в пространстве восприятия риска. Приведенные исследования позволяют предположить, что эти риски должны считаться «новыми», однако едва ли их положение будет экстремальным по осям «неизвестность» и «страх». Предположительно эти риски пока не стали частью повседневного опыта, а значит, можно ожидать высокие значения по шкале «неизвестность». Что касается страха, то наше пилотное исследование показало, что российские студенты больше всего боятся ядерной войны и терроризма [2]. И едва ли киберриски смогут значительно приблизиться к этим феноменам по измерению «страх». Скорее, наоборот, предшествующие исследования показали, что киберриски воспринимаются как контролируемые (например: [28, p. 288]), а значит, страх перед ними не может быть запредельным.

Методика

Для оценки рисков использовались 8 стандартных для «психометрической парадигмы» характеристик риска (в таблице 1 они выделены полужирным шрифтом). Помимо них, было предъявлено 4 дополнительных суждения, связанных с ответственностью разного рода субъектов за возникновение этого риска и минимизацию его последствий, однако далее мы сообщаем результаты только по 8 стандартным характеристикам. Каждый риск оценивался по этим характеристикам по семибалльной шкале.

Список рисков был основан на перечне из классической работы А. Мечитова и С. Ребрика [3]. Одновременно он был дополнен за счет высокорейтинговых рисков, выявленных по результатам исследования Н. Родионовой и ее коллег [22].

По результатам анализа литературы к перечню были добавлены следующие киберриски:

1) компьютерные игры [8];
2) информационные технологии [8];
3) мошенничество в сети Интернет [14];
4) утечка персональных данных в сети Интернет [20; 29];
5) запугивание и издевательство в киберпространстве [20; 29];
6) хакерские атаки [16];
7) компьютерные вирусы [16].

В результате использованный нами набор включал 72 риска и опасные ситуации (табл. 2).

Таблица 2

Перечень рисков, использованных в исследовании

1. *Запугивание и издевательство в киберпространстве**
2. *Информационные технологии*
3. *Компьютерные вирусы*
4. *Компьютерные игры*
5. *Мошенничество в сети Интернет*
6. *Утечка персональных данных в сети Интернет*
7. *Хакерские атаки*
8. Автомобильный транспорт
9. Альпинизм
10. Атомные электростанции
11. Беременность, роды
12. Бокс
13. Бытовые электрические инструменты
14. Вакцинация
15. Велосипеды
16. Взрывные работы
17. Взрывы в квартирах, частных домах
18. ВИЧ/СПИД
19. Война
20. Газонокосилки
21. Генная инженерия
22. Гербициды, пестициды
23. Глобальное потепление
24. Горные лыжи
25. Гражданская авиация
26. Дамбы, плотины
27. Загар, солнечные ванны
28. Заказные убийства
29. Искусственные спутники Земли
30. Использование косметики
31. Использование химических удобрений
32. Использование электрической энергии
33. Исследование космоса
34. Исследования стволовых клеток
35. Катание на роликах, роликовых досках
36. Коронавирусная инфекция COVID-19**
37. Крупнопанельное строительство
38. Курение
39. Лампы дневного освещения
40. Микроволновые печи
41. Мотоциклы
42. Наркотики
43. Незащищенный половой акт
44. Неумеренное потребление кофе
45. Обезболивающие препараты
46. Оздоровительный бег трусцой
47. Окрашивание волос
48. Опасность ядерной войны
49. Операции на сердце
50. Отдых на воде (байдарка и т. д.)
51. Охота (несчастные случаи)
52. Поездки на железных дорогах
53. Поездки на личных автомобилях
54. Пожары в зданиях
55. Потребление алкоголя
56. Преступность
57. Прием предписанных лекарств
58. Природные бедствия, катастрофы
59. Противозачаточные таблетки
60. Работа в милиции
61. Работа пожарным
62. Радиационная терапия
63. Рентген
64. Ручное огнестрельное оружие
65. Сжиженный газ (взрывы, аварии)
66. Служба в армии
67. Собирание грибов (отравление)
68. Строительство мостов, туннелей
69. Терроризм
70. Финансово-экономический кризис
71. Футбол
72. Хирургия

Примечания: * курсивом выделены киберриски; ** данный риск предъявлялся только части опрошенных, поэтому далее исключен из анализа.

Кроме того, задавались вопросы о поле, возрасте и образовании респондента, а также о приблизительном времени, затраченном на заполнение анкеты и оценку того, насколько респонденту понравилось заполнять анкету (пятибалльная шкала и вариант «затрудняюсь ответить»). В заключительном блоке была возможность оставить текстовый комментарий по анкете.

Традиционный формат исследования в «психометрической парадигме» предполагает, что респондент оценивает каждый из 72 рисков по всем суждениям и отвечает на ряд дополнительных вопросов. Анкету с таким набором суждений и рисков далее будем называть «полной».

Помимо «полной», для снижения нагрузки на респондентов использовалась также «разделенная» анкета [9]. Она включала один из 6 наборов рисков (в каждом наборе — 12 рисков), а также вопросы о социально-демографических характеристиках респондента и его оценки участия в опросе. Иными словами, каждому респонденту случайно предъявлялась одна из 6 «разделенных» анкет, где было лишь по 12 рисков. Проведенное ранее исследование показало, что в целом результаты, полученные по «полной» и «разделенной» анкетам, имеют сходную структуру, если анализировать усредненные матрицы вида «риски – характеристики» [1].

Данные

Сбор данных осуществлялся исходя из онлайн-анкеты, созданной с помощью сервиса SurveyMonkey.

Как и в большинстве предыдущих исследований, нами было принято решение использовать «конформную» выборку (convenience sample) [4; 6, с. 173–174]. Так, исходно П. Словик с коллегами использовали невероятностные выборки студентов и членов различных объединений [26], последние годы все чаще проводятся опросы онлайн, где также имеет место невероятностный отбор, например, студентов [8] или участников Amazon Mechanical Turk [13]. При «конформной» выборке полученные результаты нельзя распространить на какую-либо социальную общность, в то же время мы надеемся, что наша выборка позволит выявить некоторые существенные аспекты соотношения киберрисков и «традиционных» рисков.

Одновременно, не претендуя на валидность статистического вывода, мы постарались обеспечить гетерогенность выборочной совокупности. Для этого рекрутинг респондентов осуществлялся разными способами.

«Полную» анкету заполняли студенты департамента социологии НИУ ВШЭ. Участники исследования получали ссылку на заполнение анкеты по электронной почте. Все респонденты были слушателями курса лекций одного из авторов статьи, в качестве вознаграждения

они получали дополнительный балл к накопленной оценке за курс. В результате было собрано 149 полностью завершенных анкет, среди отвечавших — 91 девушка (61%), средний возраст — 18,4 года (SD = 0.64).

Отбор респондентов для заполнения «разделенной» анкеты осуществлялся:

1) посредством краудсорсингового проекта Яндекс.Толока 2357 респондентов заполнили анкету полностью, затратив на это 5 минут и более. Среди участников — 1243 женщины, средний возраст — 36,9 года (SD = 11.7). Респонденты получали вознаграждение 0,03 и 0,06 долл. за заполнение анкеты (267 и 2090 анкет соответственно);
2) с помощью онлайн-панели компании OMI 315 респондентов заполнили анкету полностью, затратив на это более 5 минут. Среди них — 197 женщин, средний возраст — 40,1 года (SD = 11.5). Участники получали за заполнение анкеты вознаграждение от 20 до 50 баллов во внутренней «валюте» OMI, что не превышает 75 руб. за анкету.

Таким образом, анализируемый далее массив состоял из 149 «полных» и 2672 «разделенных» анкет, заполненных до конца. Сводная таблица по участникам опроса представлена в таблице 3. Приведенная таблица свидетельствует, что наши подвыборки существенно различаются по полу и возрасту. Последующий анализ будет включать поиск различий в оценках между данными выборками: в случае незначительных различий можно надеяться, что обнаруженные особенности восприятия киберрисков имеют более универсальный характер, чем если бы они были выявлены при анализе лишь одной «конформной» выборки.

Таблица 3

Участники исследования

Способ отбора	Тип анкеты	Количество анкет*	Доля женщин, %	Средний возраст (SD)
Опрос студентов	«Полная»	149	61	14,4 (1,84)
Яндекс.Толока	«Разделенная»	2357	52	36,9 (11,7)
Онлайн-панель	«Разделенная»	300	63	40,1 (11,5)

Примечание: * после отбраковки ответов респондентов, определенных как недобросовестные.

Результаты

Как отмечалось выше, традиционно для «психометрической парадигмы» интересны поиск связей между суждениями, а также выявление факторов, определяющих пространство восприятия риска. Здесь

существуют два подхода. Первый предполагает обработку агрегированных по респондентам (чаще всего используется просто усреднение) оценок риска, то есть анализ матрицы данных вида «риск – суждение» [24]. Второй подход основывается на том, что использование лишь агрегированных значений не позволяет видеть значительную вариацию оценок на индивидуальном уровне, то есть предполагает анализ индивидуальных оценок [19]. При сборе данных мы использовали в том числе «разделенную» анкету, поэтому рассмотрение результатов на индивидуальном уровне было затруднено (по крайней мере, до тех пор, пока не будет решен вопрос о заполнении пропусков, которые, напомним, составляли 5/6 от содержательной части ответов). Исходя из этого далее следуем исключительно первому подходу к анализу результатов.

Первый проделанный шаг: сравнение средних оценок рисков по подвыборкам с целью выявления различий. По каждому риску и каждому суждению было вычислено среднеквадратическое отклонение (SD) по 3 позициям (оценка студентами, членами Яндекс.Толока и панели OMI), после этого вычислено среднее SD для 8 суждений; чем больше среднее SD, тем больше различие между выборками по данному риску. Этот показатель имеет максимальное значение у трех рисков: использование химических удобрений (0,36), курение (0,35) и утечка персональных данных в сети Интернет (0,34). Профили этих трех рисков, то есть оценки каждого риска по характеристикам, представлены на рисунке 1. По каждому суждению был проведен дисперсионный анализ (ANOVA), показавший по риску химических удобрений статистически значимые различия выборок для суждения «недобровольность риска» ($F(2, 411) = 11{,}01$, $p < 0{,}001$), «неизвестность науке» ($F(2, 411) = 3{,}57$, $p = 0{,}031$) и «новизна» ($F(2, 411) = 36{,}15$, $p < 0{,}001$). Для риска курения значимые различия наблюдаются по суждениям «неконтролируемость» ($F(2, 417) = 7{,}37$, $p < 0{,}001$) и «новизна» ($F(2, 417) = 4{,}81$, $p = 0{,}009$). Для риска утечки персональных данных в сети Интернет значимыми оказались 5 суждений: «неконтролируемость» ($F(2, 417) = 8{,}99$, $p < 0{,}001$), «отложенность воздействия» ($F(2, 417) = 3{,}32$, $p = 0{,}036$), «неизвестность науке» ($F(2, 417) = 11{,}23$, $p < 0{,}001$), «страх» ($F(2, 417) = 4{,}86$, $p = 0{,}0082$), «новизна» ($F(2, 417) = 18{,}93$, $p < 0{,}001$). Иными словами, существенные различия для большинства суждений были выявлены только по риску утечки персональных данных, тогда как в остальных случаях речь идет о различиях по отдельным суждениям. Примечательно, что профили всех рисков, в том числе риска утечки персональных данных, в целом очень похожи для наших — различающихся существенно по полу и возрасту — подвыборок. Это позволило нам далее объединить выборки и провести анализ всего массива данных.

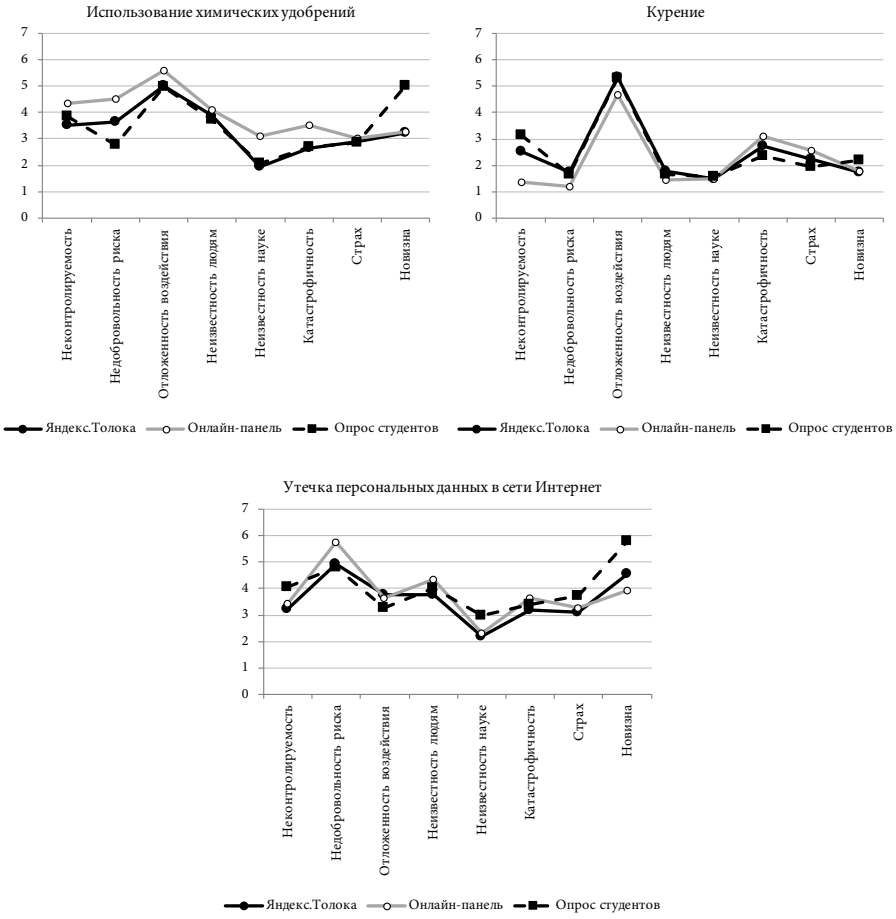

Рис. 1. Профили максимально различающихся по подвыборкам рисков

Второй — основной — шаг состоял в анализе агрегированных по всем участникам исследования оценок, представленных в виде матрицы «риск – характеристика»[2]. Если говорить о средних оценках киберрисков по суждениям, то лучше всего кибер риски позволяет дифференцировать суждение «недобровольность» (компьютерные игры как наиболее добровольный вид риска, а хакерские атаки — как наименее), а хуже всего — «неизвестность науке».

Также можно выделить некоторые особенности положения киберрисков относительно «традиционных» рисков. Во-первых, киберриски

[2] Матрица представлена в электронном Приложении к данной статье на официальном сайте СЖ по адресу: URL: https://www.jour.fnisc.ru/index.php/socjour/article/view/8649/8436

воспринимаются как менее катастрофичные ($M = 3{,}91$ для всех рисков и $M = 3{,}22$ для киберрисков), как более новые ($M = 3{,}09$ для всех рисков и $M = 4{,}81$ для киберрисков), в большей степени как не известные науке (за исключением компьютерных вирусов), но известные людям (за исключением компьютерных вирусов), $M = 2{,}33$ и $3{,}22$ для всех рисков и $M = 2{,}81$ и $3{,}84$ для киберрисков соответственно.

Содержательное сравнение оценок можно произвести посредством сопоставления профилей риска. Если в качестве меры сходства взять средний квадрат отклонений, то информационные технологии больше всего похожи на генную инженерию; компьютерные вирусы — на бытовые электрические инструменты; утечка персональных данных в сети Интернет — на гербициды и пестициды; компьютерные игры — на противозачаточные таблетки, а хакерские атаки — на хирургию. Запугивание и издевательство в киберпространстве ближе всего к радиационной терапии, а мошенничество в сети Интернет — к исследованию космоса. Примеры нескольких похожих профилей представлены на рисунке 2.

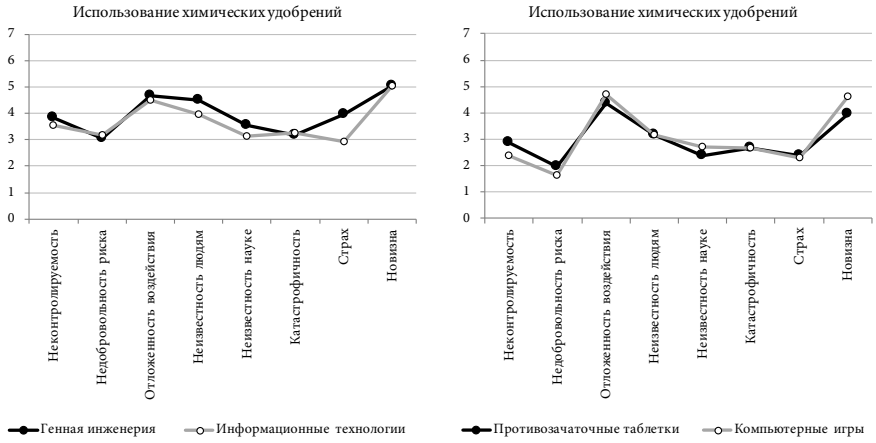

Рис. 2. Профили максимально похожих киберрисков и «традиционных» рисков

Вычисление средних от среднего квадрата отклонений показало, что ближе всего к киберрискам оказались радиационная терапия и исследование космоса.

Разумеется, изучение пространства восприятия рисков в меньшей степени предполагает рассмотрение этих частных оценок для обнаружения отдельных сходств. Вместо этого, как правило, матрица «риск – характеристика» выступает в качестве основы для проведения других методов анализа.

Перед проведением кластеризации рисков была исключена коронавирусная инфекция COVID-19, так как этот риск предъявлялся не всем респондентам. На оставшемся 71 риске был выполнен иерархиче-

ский кластерный (метод Варда, евклидово расстояние). По его результатам совокупность рисков была разбита на 6 кластеров (см. табл. 4), причем все киберриски, за исключением компьютерных игр, оказались в шестом кластере. Этот кластер характеризуется наибольшими средними значениями по суждениям «новизна», «неизвестность людям» и «неизвестность науке». Помимо 6 киберрисков, в данном кластере оказались следующие риски:

1) генная инженерия;
2) глобальное потепление;
3) искусственные спутники Земли;
4) исследование космоса;
5) исследования стволовых клеток;
6) радиационная терапия;
7) финансово-экономический кризис.

Таблица 4

Характеристика центров кластеров

Номер кластера	Количество рисков	Суждения							
		Неконтролируемость	Недобровольность риска	Отложенность воздействия	Неизвестность людям	Неизвестность науке	Катастрофичность	Страх	Новизна
1	16	2,91	2,30	2,72	2,44	2,05	4,49	2,78	2,51
2	7	2,79	2,06	4,37	2,26	1,69	2,91	2,52	2,00
3	15	3,05	2,74	4,73	3,70	2,38	2,57	2,36	3,47
4	12	4,44	5,50	2,16	3,09	2,13	5,76	4,97	2,25
5	8	3,90	4,54	3,81	3,30	2,26	4,14	3,55	2,77
6	**13**	**3,98**	**4,41**	**4,21**	**4,21**	**3,07**	**3,35**	**3,58**	**4,69**

Примечание: полужирным выделен кластер со всеми киберрисками (кроме компьютерных игр).

Если сопоставить результаты кластерного анализа с приведенным ранее попарным сравнением киберрисков и «традиционных» рисков, то окажется, что общий результат — это вывод о близости киберрисков и таких рисков, как генная инженерия и радиационная терапия.

Рассмотрим отдельно дендрограмму (метод Варда, евклидово расстояние) по 13 рискам, включенным в шестой кластер (рис. 3). Прежде всего обращает внимание наличие «пучка» из 4 киберрисков, который включает «хакерские атаки», «запугивание и издевательство

в киберпространстве», «компьютерные вирусы», «утечку персональных данных в сети Интернет».

При этом два оставшихся киберриска — «мошенничество в сети Интернет» и «информационные технологии» — вошли в состав другого «пучка». Важно, что расстояние между этими «пучками» столь значительно, что к каждому из киберрисков первого «пучка» ближе другой «пучок», включающий следующие риски: искусственные спутники Земли, глобальное потепление, экономический кризис, а к киберрискам второго «пучка» оказываются более близки такие «традиционные» риски, как радиационная терапия, исследование стволовых клеток, генная инженерия и исследование космоса.

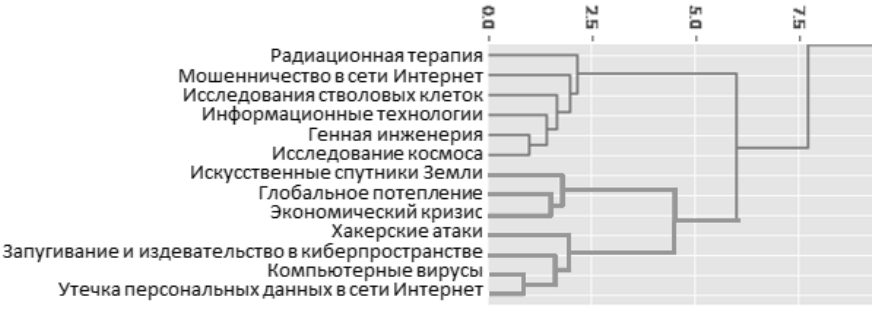

Рис. 3. Дендрограмма по 13 рискам шестого кластера

Таким образом, результаты позволяют сделать предварительный вывод, что киберриски не образуют обособленный кластер в пространстве восприятия риска: с одной стороны, киберриски могут быть подразделены на ряд подгрупп, а с другой — эти отдельные подгруппы оказались весьма близки ряду «традиционных» рисков.

В то же время в силу наличия 8 суждений содержательная интерпретация сходств и различий в значительной степени затруднена. Эта проблема интерпретации традиционно решается авторами «психометрической парадигмы» посредством использования факторного анализа. Мы также произвели уменьшение размерности данных с помощью метода главных компонент. В итоге было выявлено 2 фактора, объясняющих 81,1% общей дисперсии. В таблице 5 представлены факторные нагрузки после вращения методом Варимакс. Примечательно, что эти результаты очень точно воспроизводят картину, полученную П. Словиком и его коллегами более 30 лет назад: «отложенность воздействия», «новизна», «неизвестность людям» и «неизвестность науке» отнесены к одному фактору («неизвестность»), а все остальные суждения — к другому («страх») [24, p. 282][3]. Иными словами, факторы, по-

[3] В цитируемом исследовании использовалось 18 суждений, мы привели только те, которые совпадают с нашими характеристиками.

лученные в нашем исследовании, в целом соответствуют полученным в «классических» исследованиях в этой области.

Таблица 5

Факторные нагрузки по результатам применения метода главных компонент

Суждения	Компонент 1 («страх»)	Компонент 2 («неизвестность»)
Неконтролируемость	0,86	0,26
Недобровольность риска	0,88	0,24
Катастрофичность	0,80	–0,48
Страх	0,92	–0,01
Отложенность воздействия	–0,55	0,65
Неизвестность людям	0,21	0,91
Неизвестность науке	0,17	0,86
Новизна	–0,05	0,87

На рисунке 4 показано положение киберрисков в выявленном пространстве восприятия рисков, образованном двумя факторами — «страх» и «неизвестность».

Обращает внимание положение компьютерных игр — они воспринимаются как гораздо менее страшные по сравнению с остальными киберрисками, но при этом считаются столь же неизвестными. Положение компьютерных игр ближе всего к использованию косметики и оздоровительному бегу трусцой. Это «нестрашные» риски, с ними связывается высокая, но не чрезмерная степень неизвестности.

Остальные киберриски локализованы в области неизвестных и умеренно страшных рисков. Ближе всего к ним — если судить по среднему квадрату расстояний — гербициды и пестициды, использование химических удобрений, радиационная терапия, генная инженерия, строительство мостов и туннелей.

Примечательно, что близость информационных технологий и мошенничества в сети Интернет — одна из самых существенных, которые обнаружены в данном исследовании, что, однако, противоречит кластерному анализу, где мошенничество в сети Интернет оказалось ближе к радиационной терапии и исследованию стволовых клеток.

Таким образом, вопреки исходному предположению, киберриски не образуют локализованную и обособленную группу в пространстве восприятия риска. Даже если не принимать во внимание компьютерные игры, остальные риски занимают достаточно большую область как в восьмимерном пространстве, образованном исходными суждениями, так и в «свернутом» двумерном пространстве восприятия риска. Примерами «традиционных» рисков, занимающих сходное положение,

выступают прежде всего радиационная терапия, а также гербициды и пестициды.

Рис. 4. Положение киберрисков в пространстве восприятия рисков

Заключение

Киберриски, ключевой результат проведенного исследования, хотя достаточно близки друг к другу, не образуют отдельный кластер в пространстве восприятия рисков. Эта обособленность могла бы быть связана с экстремальными рейтингами рисков по одному из выявленных измерений. Однако, как мы и предполагали, подобные риски не вызывают значительного страха. Что касается неизвестности, то вопреки нашим ожиданиям киберриски не получили чрезвычайно высоких значений и по этому измерению, хотя и заняли «верхнюю» часть пространства восприятия. По-видимому, это связано с тем, что киберриски в значительной степени стали частью нашего повседневного опыта, по крайней мере, на уровне дискурса. Иными словами, признавая, что это сравнительно новые риски (и поэтому по оси «неизвестность» они занимают среднее положение), респонденты не боятся их, поскольку взаимодействие с ними стало привычной практикой.

Примечательно, что с точки зрения методологии «психометрической парадигмы» эти риски воспринимаются так, как генная инженерия, радиационная терапия, гербициды и пестициды. Что объединяет их? Во-первых, то, что они вызывают умеренный страх и ассоциируются с чем-то недостаточно известным. Во-вторых, можно предположить, что общее состоит в том, что все эти риски (за исключением компьютерных игр) пока неоднозначно воспринимаются как обычными людьми, так и учеными. Для такого рода рисков Дж. Адамс предлагает использовать термин «виртуальный риск» — это такой риск, относительно эффектов и вероятности которого не существует достаточного научного знания [7]. В этом смысле и киберриски и близкие им «традиционные» риски — это именно виртуальные риски: про них много говорят, они не вызывают ужаса, но одновременно отсутствует согласие относительно их влияния на жизнь индивидов и на общество в целом.

Отметим также, что в свете проведенного исследования киберриски — это, скорее, аналитический конструкт, поскольку с точки зрения обыденного восприятия между рассмотренными рисками имеются существенные различия. Также стоит учесть, что ключевым критерием отбора был «рейтинг» риска в предыдущих исследованиях, то есть мы брали только те риски, с которыми связаны наибольшие опасения и которые представлялись более значимыми, чем остальные. Это позволяет предположить, что при расширении числа киберрисков, включенных в опрос, мы, скорее всего, увидим, что эти риски окажутся еще более рассредоточенными в пространстве восприятия. В то же время существенное расширение перечня рисков затруднительно по той причине, что это значительно увеличивает затраты со стороны респондента по заполнению анкеты.

Одно из возможных решений — включить в исследование риски, руководствуясь классификацией киберрисков, то есть добавляя только «репрезентативных» представителей каждой категории. В то же время, хотя в научной литературе предложено множество различных классификаций киберрисков и смежных феноменов, например киберпреступлений (обзор классификаций см. в работе [18]), большинство из них основаны на технических различиях (например, по роли Интернета в соответствующем риске: Всемирная паутина может давать (а) больше возможностей для традиционных преступлений, (б) новые возможности для традиционных преступлений и (в) новые возможности для новых типов преступлений [31]). Как следствие, нет оснований полагать, что такие классификации релевантны именно обыденному восприятию рисков. Это значит, что перед проведением дальнейших исследований восприятия киберрисков целесообразно предложить классификацию, чувствительную именно к социальным аспектам киберрисков.

В какой мере полученные результаты могут быть генерализированы? Подчеркнем еще раз, что мы использовали невероятностную выборку, так что выводы недопустимо распространять на какие-либо реальные общности. В то же время получена достаточно высокая степень сходства в оценках на сравнительно гетерогенных подвыборках. И здесь обратим внимание, что, несмотря на существенные различия по полу и возрасту, у членов наших подвыборок есть нечто общее: они все являются активными интернет-пользователями. Хотя в нашем опросе не задавались вопросы, подтверждающие этот вывод, имеются косвенные свидетельства: студенты, будучи представителями молодежи, априори имеют самые высокие показатели цифровой грамотности [5, с. 43, 53], а что касается ОМІ и Яндекс.Толока, то использование платформ этих компаний само по себе свидетельствует об уровне цифровой компетентности участников. Иными словами, возникает соблазн распространить полученные результаты на всех интернет-пользователей или на их активную часть. Разумеется, у нас нет оснований делать такую генерализацию, однако эта специфика выборки отчасти объясняет полученные результаты: будучи активными пользователями сети Интернет, участники нашего исследования, скорее всего, знакомы с предъявляемыми киберрисками и способны их дифференцировать. Как следствие, киберриски не образовали самостоятельный кластер и «пересеклись» с многими «традиционными» рисками. Не исключено, что если бы опрашивались менее вовлеченные в цифровую среду респонденты, то оправдалась бы наша гипотеза о «компактной» локализации киберрисков в пространстве восприятия. Таким образом, в будущем целесообразно не столько попытаться использовать репрезентативную выборку, сколько включить в выборку менее активных пользователей Интернета, что позволит говорить о восприятии киберрисков «настоящими» неспециалистами, тогда как в нашем исследовании участники могут быть охарактеризованы как имеющие квазиэкспертный статус.

ЛИТЕРАТУРА

1. *Бутынко М.В., Гаврилов К.А.* Психометрическая парадигма изучения риска: опыт использования «разделенного» дизайна анкеты в онлайн-исследовании // Социология: методология, методы, математическое моделирование. 2019. № 48. С. 113–142.
2. *Гаврилов К.А.* Психометрическая парадигма в исследовании риска: перевод на русский язык и апробация на студенческой выборке // Мониторинг общественного мнения: экономические и социальные перемены. 2020. № 2. С. 33–50. DOI: 10.14515/monitoring.2020.2.761
3. *Мечитов А.И., Ребрик С.Б.* Восприятие риска // Психологический журнал. 1990. Т. 11. № 3. С. 87–95.

4. Отчет рабочей группы AAPOR о неслучайных выборках. Июнь 2013 г. Американская ассоциация исследователей общественного мнения. М.: ФОМ, 2016 [электронный ресурс]. Дата обращения 25.07.2021. URL: https://fom.ru/uploads/files/FOM_AAPOR_book1.pdf
5. Оценка цифровой готовности населения России. Доклад к XXII Апрельской международной научной конференции по проблемам развития экономики и общества. Москва, 13–30 апреля 2021 г. / Н.Е. Дмитриева и др. М.: НИУ ВШЭ, 2021 [электронный ресурс]. Дата обращения 25.07.2021. URL: https://conf.hse.ru/mirror/pubs/share/464963752.pdf
6. *Чуриков А.В.* Основы построения выборки для социологических исследований. М.: ФОМ, 2020. — 240 с.
7. *Adams J.* Cars, Cholera, and Cows. The Management of Risk and Uncertainty // Policy Analysis. 1999. No. 335. P. 1–49.
8. *Bassarak C., Pfister H.-R., Böhm G.* Dispute and morality in the perception of societal risks: extending the psychometric model // Journal of Risk Research. 2017. Vol. 20 (3). P. 299–325. DOI: 10.1080/13669877.2015.1043571
9. *Bronfman N., Cifuentes L.* Risk Perception in a Developing Country: The Case of Chile // Risk Analysis. 2003. Vol. 23 (6). P. 1309–1324. DOI: 10.1111/j.0272-4332.2003.00400.x
10. *Bronfman N., Cifuentes L., deKay M., Willis H.* Accounting for Variation in the Explanatory Power of the Psychometric Paradigm: The Effects of Aggregation and Focus // Journal of Risk Research. 2007. Vol. 10. No. 4. P. 527–554. DOI: 10.1080/13669870701315872
11. *Chauvin B., Hermand D.* Contribution du Paradigme Psychométrique à l'étude de la perception des risques: une revue de la littérature de 1978 à 2005 // L'Année Psychologique. 2008. Vol. 108. P. 343–386. DOI: 10.4074/S0003503308002066
12. *Fishhoff B., Slovic P., Lichtenstein S., Read S., Combs B.* How Safe is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits // Policy Sciences. 1978. Vol. 9. P. 127–152. DOI: 10.1007/BF00143739
13. *Fox-Glassman K., Weber E.* What makes risk acceptable? Revisiting the 1978 psychological dimensions of perceptions of technological risks // Journal of Mathematical Psychology. 2016. Vol. 75. P. 157–169. DOI: 10.1016/j.jmp.2016.05.003
14. *Garg V., Camp L.* End User Perception of Online Risk under Uncertainty // 45th Hawaii International Conference on System Sciences. Hawaii, 2012. P. 3278–3287. DOI: 10.1109/HICSS.2012.245
15. *Gaudenzi B., Siciliano G.* Just do it: Managing IT and Cyber Risks to Protect the Value Creation // Journal of Promotion Management. 2017. Vol. 23. No. 3. P. 372–385. DOI: 10.1080/10496491.2017.1294875
16. *Huang D.-L., Rau P.-L., Salvendy G.* Perception of information security // Behaviour & Information Technology. 2010. Vol. 29. No. 3. P. 221–232. DOI: 10.1080/01449290701679361

17. *Jackson J., Allum N., Gaskell G.* Perceptions of Risk in Cyberspace // Trust and Crime in Information Societies / Ed. by R. Mansell, B. Collins. Cheltenham: Edward Elgar, 2005. P. 245–281.
18. *Jahankhani H., Al-Nemrat A., Hosseinian-Far A.* Cybercrime classification and characteristics // Cyber Crime and Cyber Terrorism Investigator's Handbook / Ed. by B. Akhgar, A. Staniforth, F. Bosco. Waltham: Syngress, 2014. P. 149–164. DOI: 10.1016/B978-0-12-800743-3.00012-8
19. *Marris C., Langford I., Saunderson T., O'Riordan T.* Exploring the "Psychometric Paradigm": Comparisons Between Aggregate and Individual Analyses // Risk Analysis. 1997. Vol. 17. P. 303–312. DOI: 10.1111/j.1539-6924.1997.tb00868.x
20. *Oliveira E., Baldi V.* Perception of Risk and Precautionary Behavior in CyberSecurity: Hints for Future Research // Proceedings of the Digital Privacy and Security Conference. 2019. P. 28–38.
21. *Ramos-Soler I., López-Sánchez C., Torrecillas-Lacave T.* Online risk perception in young people and its effects on digital behavior // Comunicar. 2018. Vol. 26 (56). P. 71–79. DOI: 10.3916/C56-2018-07
22. *Rodionova N., Vinsonneau G., Rivière S., Mullet E.* Societal Risk Perception in Present Day Russia // Human and Ecological Risk Assessment: An International Journal. 2009. Vol. 15 (2). P. 388–400. DOI: 10.1080/10807030902761486
23. *Siegrist M., Keller C., Kiers H.* A New Look at the Psychometric Paradigm of Perception of Hazards // Risk Analysis. 2005. Vol. 25. No. 1. P. 211–222. DOI: 10.1111/j.0272-4332.2005.00580.x
24. *Slovic P.* Perception of Risk // Science. 1987. Vol. 236. P. 280–285. DOI: 10.1126/science.3563507
25. *Slovic P.* The Perception of Risk. London: Earthscan, 2000. — 511 p.
26. *Slovic P., Fischhoff B., Lichtenstein S.* Characterizing Perceived Risk // Perilous Progress: Managing the Hazards of Technology / Ed. by R. Kates, C. Hohenemser, J. Kasperson. Boulder: Westview, 1985. P. 91–125.
27. *Van Loon J.* Risk and Technological Culture: Towards a Sociology of Virulence. London: Routledge, 2002. — 245 p. DOI: 10.4324/9780203466384
28. *Van Schaik P., Jansen J., Onibokun J., Camp J., Kusev P.* Security and privacy in online social networking: Risk perceptions and precautionary behavior // Computers in Human Behavior. 2018. Vol. 78. P. 283–297. DOI: 10.1016/j.chb.2017.10.007
29. *Van Schaik P., Jeske D., Onibokun J., Coventry L., Jansen J., Kusev P.* Risk perceptions of cyber-security and precautionary behavior // Computers in Human Behavior. 2017. Vol. 75. P. 547–559. DOI: 10.1016/j.chb.2017.05.038
30. *Von Solms R., van Niekerk J.* From information security to cyber security // Computers & Security. 2013.Vol. 38. P. 97–102. DOI: 10.1016/j.cose.2013.04.004
31. *Wall D.S.* The Internet as a Conduit for Criminal Activity // Information technology and the criminal justice system / Ed. by A. Pattavina. Thousand Oaks: Sage Publications, Inc., 2005 [online]. Accessed 25.07.2021. URL: https://ssrn.com/abstract=740626

СВЕДЕНИЯ ОБ АВТОРАХ

Гаврилов Кирилл Андреевич — кандидат социологических наук, доцент, кафедра анализа социальных институтов, НИУ «Высшая школа экономики»; научный сотрудник, Институт социологии ФНИСЦ РАН. **Телефон:** +7 (910) 413-56-14. **Электронная почта:** gavrilov@socio.msk.ru

Бутынко Мария Викторовна — аналитик, ГКУ «Информационный город». **Телефон:** +7 (964) 789-67-39. **Электронная почта:** butynko.maria@yandex.ru

Дата поступления: 18.02.2021.

Sotsiologicheskiy Zhurnal = Sociological Journal. 2021. Vol. 27. No. 4. P. 146–168. DOI: 10.19181/socjour.2021.27.4.8649

Research Article

***Kirill A. Gavrilov*[1, 2], *Mariya V. Butynko*[3]**

[1] National Research University Higher School of Economics.
20, Myasnitskaya str., 101000, Moscow, Russian Federation.

[2] Institute of Sociology of FCTAS RAS.
5, bl. 1, Bolshaya Andronievskaya str., 109544, Moscow, Russian Federation.

[3] GKU Infogorod.
5, bl. 16, Nizhniy Susalny per., 105064, Moscow, Russian Federation.

The Perception of Cyber and Traditional Risks: Experience of Using the Psychometric Paradigm Approach

Abstract. This article presents the results of using the "psychometric paradigm" methodology (P. Slovic, B. Fischhoff, S. Lichtenstein and others) to study the perception of cyber risks and compare them to other risks designated as "traditional". The respondents in an online survey were presented seven cyber risks (from computer games to hacker attacks and viruses) and 65 traditional risks (from natural disasters to nuclear power plants and terrorism), assessed based on 8 characteristics. As a result, computer games were perceived differently compared to other cyber risks: first of all, they do not induce fear. Other cyber risks are concentrated in an area of relatively obscure and moderately frightening risks, but they do not form a separate cluster. Radiation therapy, herbicides and pesticides are the closest to cyber risks in the two-dimensional space of risk perception. The results of this pilot survey may be considered a reflection of the sample used, where the main participants were active Internet users who were able to distinguish between the presented cyber risks.

Keywords: cyber risks; risk; risk perception; psychometric paradigm.

For citation: Gavrilov, K.A., Butynko, M.V. The Perception of Cyber and Traditional Risks: Experience of Using the Psychometric Paradigm Approach. *Sotsiologicheskiy Zhurnal = Sociological Journal.* 2021. Vol. 27. No. 4. P. 146–168. DOI: 10.19181/socjour.2021.27.4.8649

REFERENCES

1. Butynko M.V., Gavrilov K.A. Psychometric Paradigm in Risk Research: an Experience of Using the Split Questionnaire Design in an Online Survey. *Sotsiologiya 4M (Sociology: methodology, methods, mathematical modeling)*. 2019. No. 48. P. 113–142. (In Russ.)

2. Gavrilov K.A. Psychometric paradigm in risk research: a translation into Russian and a pilot study with a student sample *Monitoring obshchestvennogo mneniya: ekonomicheskie i sotsial'nye peremeny*. 2020. No. 2. P. 33–50. (In Russ.)
3. Mechitov A.I., Rebrik S.B. Risk perception. *Psikhologicheskii zhurnal*. 1990. No. 11 (3). P. 87–95. (In Russ.)
4. *Otchet rabochei gruppy AAPOR o nesluchainykh vyborkakh. Iyun' 2013 g. Amerikanskaya assotsiatsiya issledovatelei obshchestvennogo mneniya*. [Report of the AAPOR task force on nonprobability sampling.] Transl. from Eng. Moscow: FOM publ., 2016. Accessed 25.07.2021. URL: https://fom.ru/uploads/files/FOM_AAPOR_book1.pdf (In Russ.)
5. *Otsenka tsifrovoi gotovnosti naseleniya Rossii. Doklad k XXII Aprel'skoi mezhdunarodnoi nauchnoi konferentsii po problemam razvitiya ekonomiki i obshchestva. Moskva, 13–30 aprelya 2021 g.* [Assessment of the digital readiness of the population of Russia. Report for the XXII Apr. international scientific conference on the problems of economic and social development. Moscow. 13–30 April 2021.] Ed. by N. Dmitrieva, et al. Moscow: NRU HSE publ., 2021. Accessed 25.07.2021. URL: https://conf.hse.ru/mirror/pubs/share/464963752.pdf (In Russ.)
6. Churikov A. *Osnovy postroeniya vyborki dlya sotsiologicheskikh issledovanii*. [Basics of sampling for sociological research.] Moscow: FOM publ., 2020. (In Russ.)
7. Adams J. Cars, Cholera, and Cows. The Management of Risk and Uncertainty. *Policy Analysis*. 1999. No. 335. P. 1–49.
8. Bassarak C., Pfister H.-R., Böhm G. Dispute and morality in the perception of societal risks: extending the psychometric model. *Journal of Risk Research*. 2017. No. 20 (3). P. 299–325. DOI: 10.1080/13669877.2015.1043571
9. Bronfman N., Cifuentes L. Risk Perception in a Developing Country: The Case of Chile. *Risk Analysis*. 2003. No. 23 (6). P. 1309–1324. DOI: 10.1111/j.0272-4332.2003.00400.x
10. Bronfman N., Cifuentes L., deKay M., Willis H. Accounting for Variation in the Explanatory Power of the Psychometric Paradigm: The Effects of Aggregation and Focus. *Journal of Risk Research*. 2007. No. 10 (4). P. 527–554. DOI: 10.1080/13669870701315872
11. Chauvin B., Hermand D. Contribution du Paradigme Psychométrique à l'étude de la perception des risques: une revue de la littérature de 1978 à 2005. *L'Année Psychologique*. 2008. No. 108. P. 343–386. DOI: 10.4074/S0003503308002066
12. Fishhoff B., Slovic P., Lichtenstein S., Read S., Combs B. How Safe is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits. *Policy Sciences*. 1978. No. 9. P. 127–152. DOI: 10.1007/BF00143739
13. Fox-Glassman K., Weber E. What makes risk acceptable? Revisiting the 1978 psychological dimensions of perceptions of technological risks. *Journal of Mathematical Psychology*. 2016. No. 75. P. 157–169. DOI: 10.1016/j.jmp.2016.05.003
14. Garg V., Camp L. *End User Perception of Online Risk under Uncertainty, 45th Hawaii International Conference on System Sciences*. Hawaii, 2012. P. 3278–3287. DOI: 10.1109/HICSS.2012.245
15. Gaudenzi B., Siciliano G. Just do it: Managing IT and Cyber Risks to Protect the Value Creation. *Journal of Promotion Management*. 2017. No. 23 (3). P. 372–385. DOI: 10.1080/10496491.2017.1294875
16. Huang D.-L., Rau P.-L., Salvendy G. Perception of information security. *Behaviour & Information Technology*. 2010. No. 29 (3). P. 221–232. DOI: 10.1080/01449290701679361
17. Jackson J., Allum N., Gaskell G. Perceptions of Risk in Cyberspace. *Trust and Crime in Information Societies*. Ed. by R. Mansell, B. Collins. Cheltenham: Edward Elgar, 2005. P. 245–281.
18. Jahankhani H., Al-Nemrat A., Hosseinian-Far A. Cybercrime classification and characteristics. Akhgar B., Staniforth A., Bosco F. (eds) *Cyber Crime and Cyber Terrorism*

Investigator's Handbook. Waltham: Syngress, 2014. P. 149–164. DOI: 10.1016/B978-0-12-800743-3.00012-8
19. Marris C., Langford I., Saunderson T., O'Riordan T. Exploring the "Psychometric Paradigm": Comparisons Between Aggregate and Individual Analyses. *Risk Analysis*. 1997. Vol. 17. P. 303–312. DOI: 10.1111/j.1539-6924.1997.tb00868.x
20. Oliveira E., Baldi V. Perception of Risk and Precautionary Behavior in CyberSecurity: Hints for Future Research. *Proceedings of the Digital Privacy and Security Conference*. 2019. P. 28–38.
21. Ramos-Soler I., López-Sánchez C., Torrecillas-Lacave T. Online risk perception in young people and its effects on digital behaviour. *Comunicar*. 2018. No. 26 (56). P. 71–79. DOI: 10.3916/C56-2018-07
22. Rodionova N., Vinsonneau G., Rivière S., Mullet E. Societal Risk Perception in Present Day Russia. *Human and Ecological Risk Assessment: An International Journal*. 2009. No. 15 (2). P. 388–400. DOI: 10.1080/10807030902761486
23. Siegrist M., Keller C., Kiers H. A New Look at the Psychometric Paradigm of Perception of Hazards. *Risk Analysis*. 2005. No. 25 (1). P. 211–222. DOI: 10.1111/j.0272-4332.2005.00580.x
24. Slovic P. Perception of Risk. *Science*. 1987. No. 236. P. 280–285. DOI: 10.1126/science.3563507
25. Slovic P. *The Perception of Risk*. L.: Earthscan, 2000. 511 p.
26. Slovic P., Fischhoff B., Lichtenstein S. Characterizing Perceived Risk. *Perilous Progress: Managing the Hazards of Technology*. Ed. by R. Kates., C. Hohenemser, J. Kasperson. Boulder: Westview, 1985. P. 91–125.
27. Van Loon J. *Risk and Technological Culture: Towards a Sociology of Virulence*. L.: Routledge, 2002. 245 p. DOI: 10.4324/9780203466384
28. Van Schaik P., Jansen J., Onibokun J., Camp J., Kusev P. Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*. 2018. No. 78. P. 283–297. DOI: 10.1016/j.chb.2017.10.007
29. Van Schaik P., Jeske D., Onibokun J., Coventry L., Jansen J., Kusev P. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*. 2017. No. 75. P. 547–559. DOI: 10.1016/j.chb.2017.05.038
30. Von Solms R., van Niekerk J. From information security to cyber security. *Computers & Security*. 2013. No. 38. P. 97–102. DOI: 10.1016/j.cose.2013.04.004
31. Wall D.S. The Internet as a Conduit for Criminal Activity. *Information technology and the criminal justice system*. Ed. by A. Pattavina. Thousand Oaks: Sage Publications, 2005. Accessed 25.07.2021. URL: https://ssrn.com/abstract=740626

Information about the authors

Kirill A. Gavrilov — Candidate of Sociological Sciences, Research Fellow, Institute of Sociology of FCTAS RAS; Associate Professor, NRU Higher School of Economics. **Phone:** +7 (910) 413-56-14. **Email:** gavrilov@socio.msk.ru

Maria V. Butynko — Analyst, GKU Infogorod. **Phone:** +7 (964) 789-67-39. **Email:** butynko.maria@yandex.ru

Received: 18.02.2021.