Психология и право
2021. Том 11. № 4. С. 207—220.
DOI: https://DOI.org/10.17759/psylaw.2021110415
ISSN: 2222-5196 (online)

Psychology and Law
2021. Vol. 11, no. 4, pp. 207—220.
DOI: https:///DOI.org/10.17759/psylaw.2021110415
ISSN: 2222-5196 (online)

МЕЖДИСЦИПЛИНАРНЫЕ ИССЛЕДОВАНИЯ | INTERDISCIPLINARY STUDIES

Культура информационной безопасности: психолого-правовой аспект

Бегишев И.Р.
Казанский инновационный университет имени В.Г. Тимирясова (КИУ им. В.Г. Тимирясова), г. Казань, Российская Федерация
ORCID: https://orcid.org/0000-0001-5619-4025, e-mail: begishev@mail.ru

Цифровые технологии стали неотъемлемой частью современной деятельности человека. Сегодня они проникают во все сферы деловой и личной жизни. Большинству организаций для развития и процветания нужны информационные системы, и поэтому они должны серьезно относиться к защите своих цифровых активов. Многие процессы, необходимые для обеспечения безопасности цифровых активов, в значительной степени зависят от взаимодействия человека. В работе предпринята попытка осветить культуру информационной безопасности сквозь призму психологии и права. Результаты исследования показали, что с психологической точки зрения культура информационной безопасности включает готовность современного человека к преодолению цифровой экспансии за счет овладения им инструментарием противодействия негативным информационным факторам. В свою очередь, с правовой точки зрения культура информационной безопасности базируется на нормативно-правовой базе, регулирующей правоотношения в сфере кибербезопасности.

Ключевые слова: информационная безопасность, информационно-психологическая безопасность, киберпсихология, культура, социальная инженерия, угроза, цифровая экспансия, человеческий фактор.

Для цитаты: *Бегишев И.Р.* Культура информационной безопасности: психолого-правовой аспект [Электронный ресурс] // Психология и право. 2021. Том 11. № 4. С. 207—220. DOI:10.17759/psylaw.2021110415

Cyber-Security Culture: Psychological and Legal Aspects

Ildar R. Begishev
Kazan Innovative University named after V.G. Timiryasov, Kazan, Russian Federation
ORCID: https://orcid.org/0000-0001-5619-4025, e-mail: begishev@mail.ru

Digitalization has become part and parcel of the modern-day human activities. Nowadays it is going into every field of business and personal life. To develop and prosper, most organizations need IT systems, and hence to take the safeguarding of their informational assets seriously. Many of the processes which are essential for securing their IT assets, largely depend on human interaction. This study has attempted to address the culture of cyber-security in the light of psychology and law. The results of the research showed that from the psychological standpoint, the culture of cyber-security involves the willingness on the part of a modern human to overcome the digital expansion by mastering the tools for countering the negative IT factors. In its turn, from the legal standpoint, the culture of cyber-security is based on the legislative framework which regulates the legal relations in the field of cyber-security.

Keywords: cyber-security, informational and psychological security, cyberpsychology, culture, social engineering, threat, digital expansion, human factor.

For citation: Begishev I.R. Cyber-Security Culture: Psychological and Legal Aspects. *Psikhologiya i pravo = Psychology and Law*, 2021. Vol. 11, no. 4, pp. 207—220. doi:10.17759/psylaw.2021110415 (In Russ.).

В современном обществе объем информационных потоков имеет постоянную тенденцию к росту. В этой связи цифровая информация выступает важным, дорогостоящим активом, который часто становится предметом посягательства со стороны злоумышленников. Основная опасность указанного посягательства заключена в том, что при несанкционированном доступе к цифровой информации, цель которого незаконное завладение ею, под угрозой может находиться безопасность личности, общества и государства [19]. Следовательно, одной из важных проблем становится задача обеспечения информационной безопасности.

Необходимо также отметить комплексность проблемы обеспечения информационной безопасности. Существует мнение, что для обеспечения информационной безопасности достаточно создания мощной программной или технической защиты, которая ограничит нежелательный доступ посторонних лиц к цифровой информации. Однако это не совсем верно. Обеспечить информационную безопасность как на макро-, так и на микроуровне только техническими средствами невозможно, равно как и только при помощи мер, предпринимаемых правоохранительными органами. Необходимо, чтобы все участники информационных процессов осознали необходимость и важность информационной безопасности для общества, учитывали факторы, которые создают угрозу безопасности, понимали свою ответственность и роль в обеспечении информационной безопасности и по необходимости принимали меры по повышению безопасности цифровой информации, цифровой инфраструктуры и цифровых технологий. Все вышесказанное и составляет основу культуры информационной безопасности.

Рассмотрим составляющие данного понятия. Непосредственно культура являет собой совокупность нравственных, моральных и материальных ценностей, умений, знаний, а также обычаев и традиций. Кроме того, культуру именуют также определенной формой деятельности, или процессом создания, и в качестве результата вышеозначенного выступает

комплекс нравственных, моральных и материальных ценностей.

В свою очередь, информационная безопасность — категория двоякая — она включает информационно-психологическую безопасность, обеспечивающую защищенность субъектов от негативных информационных воздействий, и безопасность информации, которая обеспечивает защиту непосредственно информации. Указанные составляющие информационной безопасности во многом определяют сущность культуры информационной безопасности [16].

В работе [29] культура информационной безопасности определяется с академической и отраслевой точек зрения. Результаты исследования показали, что научные интерпретации определений и факторов культуры информационной безопасности намного шире, чем их понимание в отрасли кибербезопасности.

Кроме того, некоторые ученые утверждают, что необходимо изучить культуру информационной безопасности различных профессиональных сообществ [39].

Статья [30] освещает вопросы исследования концепции культуры информационной безопасности и то, как конфиденциальность информации может быть включена в определение культуры защиты информации. Культура информационной безопасности является предиктором конфиденциальности информации.

В исследованиях [38; 41; 44] применена оценка отношений между культурой безопасности и информационной безопасностью. Выводы исследований говорят о том, что организации должны сосредоточиться на культуре информационной безопасности, чтобы улучшить состояние информационной безопасности, экономя при этом время и ресурсы.

Можно согласиться с точкой зрения А. Мартинса и Я. Элофе, считающих, что в каждой организации культура информационной безопасности зависит от того, как люди ведут себя по отношению к информации и ее безопасности. Процедуры, которые сотрудники используют в своей повседневной деятельности, могут представлять собой самое слабое звено в цепочке информационной безопасности. Поэтому важно развивать и совершенствовать культуру информационной безопасности через структурированную модель, учитывающую поведение сотрудников [34].

К аналогичной точке зрения на природу рассматриваемого феномена приходят Т. Шлингер и С. Тойфель в работе «Культура информационной безопасности. Социокультурное измерение в управлении информационной безопасностью». Они объясняют концепцию корпоративной культуры на примере культуры информационной безопасности организации, выдвигая теорию смещения парадигмы с технического подхода на социокультурный, с подхода «пользователь — мой враг» к подходу «пользователь — мой актив безопасности» [40].

Не следует забывать, что большинство нарушений безопасности являются результатом человеческих ошибок. Для того чтобы организации могли повысить свою кибербезопасность и обеспечить более качественную подготовку своих сотрудников к противодействию киберугрозам, они должны исследовать понимание человеческих ошибок, типов человеческих ошибок, что делает их основной причиной нарушений, а также способы уменьшения их количества [23]. Человеческий фактор является основной причиной угроз информационной безопасности в организациях [25]. Широко признано, что создание организационной субкультуры информационной безопасности является ключом к управлению человеческими факторами, вовлеченными в информационную безопасность [43].

Эксперты подчеркивают важность сотрудников в стратегиях противодействия киберпреступности, учитывая, что людей часто считают самым слабым звеном в цепи безопасности. Фактически международные отчеты, анализирующие кибератаки, подтверждают, что основная проблема представлена действиями сотрудников, например, открытием фишинговых писем и непроверенных вложенных файлов, передачей конфиденциальной информации посредством атак социальной инженерии. Следует признать, что сотрудники, если они хорошо подготовлены, являются первой защитной линией в организации. Следовательно, в любом образовательном плане по кибербезопасности первостепенным шагом является анализ восприятия рисков людьми с целью разработки индивидуальной программы обучения [27].

Используя эффективные образовательные программы, сотрудники организаций могут быть обучены тому, как принимать безопасные решения. Для успеха программы крайне важно, чтобы сотрудники были обучены надлежащим образом, поскольку они являются основным уровнем защиты от неправомерных действий и стали бесценной частью общей стратегии информационной безопасности организации [33]. К тому же образовательные программы в сфере информационной безопасности необходимы для выработки сотрудниками представления о способах и средствах обеспечения безопасности информации. Основная цель этих программ — формирование позитивной культуры информационной безопасности в организации [31].

Современные организации работают во взаимосвязанной и глобальной цифровой среде, что позволяет им сотрудничать друг с другом и обмениваться цифровой информацией. В то же время эта взаимосвязанность подвергает организацию множеству внутренних и внешних угроз. Внутренняя угроза является одной из главных проблем информационной безопасности, с которой сталкиваются организации [37]. Сотрудники, умышленно или по неосторожности, часто из-за недостатка знаний, представляют наибольшую угрозу информационной безопасности.

В области кибербезопасности человеческий фактор считается одним из важнейших элементов. Эксперты по безопасности хорошо знают важность таких мер безопасности, как управление паролями, предотвращение фишинговых атак и т. п. Однако организациям по-прежнему не хватает сильной культуры кибербезопасности для управления рисками безопасности, связанными, в частности, с человеческим фактором. Компьютерные атаки, основанные на методах социальной инженерии, считаются одними из самых успешных, поскольку используют психологические принципы для манипулирования восприятием людей и получения ценной информации [28].

Проблема манипулирования людьми с помощью различных методов социальной инженерии и технологий информационно-психологической войны стала массовым явлением и представляет собой серьезную угрозу информационно-психологической безопасности личности [45]. При этом основная суть манипуляции человеком сводится к скрытому психологическому принуждению личности.

Соблюдение каждым сотрудником требований информационной безопасности носит индивидуальный характер и ставится в зависимость от его индивидуальных психологических особенностей. Оно опосредовано таким аттитюдом, как устойчивое субъективное отношение сотрудников к политике информационной безопасности организации, к правилам защиты информации, к своим должностным обязанностям. Строгая дисциплина и культура информационной безопасности являются ключевым фактором в деле обеспечения

информационной безопасности [3, с. 63—64].

Кроме того, низкий уровень культуры информационной безопасности (недостаточная осведомленность руководителей и специалистов организаций в вопросах обеспечения информационной безопасности, игнорирование сотрудниками требований политики информационной безопасности организации, несоблюдение сотрудниками требований федерального законодательства в сфере информационной безопасности и т. д.) является причиной синдрома безопасной атаки — состояния субъектов информационных правоотношений, осознающих опасность нарушения и важность обеспечения безопасности информационной инфраструктуры, но в силу различных причин не обеспечивающих ее, в том числе при проведении в отношении нее компьютерных атак [1, с. 30].

По мнению австралийских ученых из психологической школы Университета Аделаиды, для успешного принятия решений в области информационной безопасности необходимы знание и соблюдение политик информационной безопасности, правовое поведение сотрудников [38].

Таким образом, знание сотрудниками того, какие политики и процедуры информационной безопасности они должны соблюдать, их понимание того, почему они должны придерживаться правил и что они на самом деле делают (своего поведения), может положительно повлиять на состояние защищенности цифровой информации и цифровой инфраструктуры [35].

Исследователи из малазийского университета акцентируют внимание на том, что организации выиграют от мониторинга информационной безопасности, поощряя поведение сотрудников, выходящее за рамки политики безопасности. Они уверены, что некоторые сотрудники склонны отказываться от безопасных действий, когда такое поведение воспринимается как неудобное. Следовательно, организации должны найти способы уменьшить воспринимаемые неудобства, используя различные методы автоматизации информационной безопасности и специализированные программы обучения [22], поскольку создание позитивной культуры информационной безопасности — это эффективный способ пропаганды поведения и практики безопасности среди сотрудников организации [36].

Существует мнение, что культура информационной безопасности определяет порядок действий в организации в отношении информационной безопасности с целью защиты информационных активов и влияния на безопасность сотрудников [24].

Весьма полезными для нас оказались результаты исследований зарубежных ученых, которые при изучении связи между кибербезопасностью и культурными, личностными и демографическими переменными выявили закономерности и пришли к выводу, что культура, поведение, самоэффективность и отношение к частной жизни оказывают влияние на культуру информационной безопасности по сравнению с другими психологическими и демографическими переменными [32], в том числе при решении проблемы апатии сотрудников к информационной безопасности [42]. Подход организации к информационной безопасности должен быть ориентирован на поведение сотрудников, поскольку успех организации сильно зависит от того, что и как ее сотрудники делают.

Таким образом, культура информационной безопасности в психологическом аспекте включает такую составляющую, как информационно-психологическая безопасность. Так, известно, что сегодня информационное воздействие может негативно влиять на психические функции как отдельно взятого человека, так и массы людей. Это, в свою очередь, негативно отражается на реализации жизненно важных интересов личности, общества и государства в

цифровой сфере.

В литературе существует мнение, что информационные технологии сегодня — это центральная угроза информационно-психологической безопасности личности [15]. Средства массовой информации способны формировать сознание современного человека. Кроме того, нельзя недооценивать влияния на психику различных ресурсов информационно-телекоммуникационной сети «Интернет». Например, дети и подростки, психика которых подвержена различным воздействиям, испытывают на себе особенно сильное влияние цифровых потоков информации [4—8; 10—14; 18; 20; 21; 26].

Сегодня в информационно-телекоммуникационной сети «Интернет» получают распространение пропагандистские материалы [9], фейковые новости [17] и призывы для вовлечения в организованную преступную деятельность [2, с. 97], публикуются рецепты изготовления взрывчатых веществ, оружия, наркотиков и пр. Подобная информация может иметь научно-технический характер, а может представлять серьезную угрозу для национальной безопасности и в отдельных случаях причинять вред психическому здоровью граждан.

Некоторая часть граждан также безосновательно считают, что правонарушения, которые они совершают в информационно-телекоммуникационной сети «Интернет», будут носить характер анонимности и, соответственно, останутся безнаказанными. Именно поэтому, будучи в жизни законопослушными гражданами, в информационно-телекоммуникационной сети «Интернет» они могут проявлять свои агрессивные противоправные наклонности.

Обществу и государству необходимо принять ряд мер, чтобы защитить как молодое, так и старшее поколение от негативного влияния цифровых потоков, которое может проявиться психическими нарушениями, возникновением психоэмоциональных проблем.

Культура информационной безопасности способна обеспечить устойчивость психики личности к различным информационным воздействиям. В связи с этим уровень культуры информационной безопасности личности будет определяться ее способностью произвести критический анализ, оценить воспринимаемую информацию для принятия объективного решения с учетом этих данных.

Посредством формирования и развития культуры информационной безопасности возможно преодоление цифровой экспансии. Осознавая всю глубину проблемы, люди должны быть готовы к глобальным цифровым переменам, событиям, в качестве участников которых им приходится выступать. На этом пути важным этапом может стать разработка теории цифровых нововведений, так как часто готовность граждан к новшествам при формировании цифрового общества оставляет желать лучшего. Кроме того, владеющий культурой информационной безопасности гражданин должен быть знаком с психологическими аспектами принятия стратегических решений в условиях цифровой экономики.

В то же время с правовой точки зрения культура информационной безопасности — это знания и навыки граждан, в том числе и тех, кто находится при исполнении профессиональных обязанностей в сфере защиты информационных и киберфизических систем.

Центральная составляющая культуры информационной безопасности — это совокупность политик информационной безопасности, правил, норм и стандартов безопасного использования цифровых технологий, в том числе этические нормы.

Государственно-правовая политика в рамках формирования культуры информационной

безопасности основана на дифференцировании мероприятий государственной политики по основным социальным группам общества, для того чтобы преодолеть недостаток знаний в цифровой сфере, а также на координации деятельности государственных органов, бизнес-структур и институтов гражданского общества путем разработки и принятия соответствующих правовых актов.

В заключение отметим, что культура информационной безопасности может быть рассмотрена как в психологическом, так и в правовом разрезе. С психологической точки зрения культура информационной безопасности включает готовность современного человека к преодолению цифровой экспансии за счет овладения им инструментарием противодействия негативным информационным факторам. С правовой точки зрения культура информационной безопасности базируется на нормативно-правовой базе, регулирующей правоотношения в сфере кибербезопасности.

Литература

1. *Бегишев И.Р.* Синдром безопасной атаки: юридико-психологический феномен // Юридическая психология. 2018. № 2. С. 27—30.
2. *Бегишев И.Р., Хисамова З.И., Никитин С.Г.* Организация хакерского сообщества: криминологический и уголовно-правовой аспекты // Всероссийский криминологический журнал. 2020. Том 14. № 1. С. 96—105. doi:10.17150/2500-4255.2020.14(1)
3. *Бегишев И.Р., Бикеев И.И.* Преступления в сфере обращения цифровой информации. Казань: Изд-во «Познание» Казанского инновационного университета, 2020. 300 с.
4. *Бовина И.Б., Дворянчиков Н.В., Будыкин С.В.* Информационная безопасность детей в обыденном понимании родителей и учителей // Вестник Российского университета дружбы народов. Серия: Психология и педагогика. 2016. № 1. С. 77—86.
5. *Бовина И.Б., Дворянчиков Н.В., Гаямова С.Ю., Милёхин А.В., Будыкин С.В.* Социальные представления и информационная безопасность детей и подростков: точка зрения учителей (Часть 1) [Электронный ресурс] // Психология и право. 2017. Том 7. № 1. С. 1—12. doi: 10.17759/psylaw.2017070101
6. *Бовина И.Б., Дворянчиков Н.В., Гаямова С.Ю., Милёхин А.В., Будыкин С.В.* Социальные представления и информационная безопасность детей и подростков: точка зрения учителей (Часть 2) [Электронный ресурс] // Психология и право. 2017. Том 7. № 2. С. 19—32. doi:10.17759/psylaw.2017060202
7. *Бовина И.Б., Дворянчиков Н.В., Гаямова С.Ю., Милёхин А.В., Будыкин С.В.* Социальные представления и информационная безопасность детей и подростков: точка зрения учителей (Часть 3) [Электронный ресурс] // Психология и право. 2017. Том 7. № 3. С. 138—148. doi:10.17759/psylaw.2017070311
8. *Бовина И.Б., Дворянчиков Н.В., Будыкин С.В.* Информационная безопасность детей и подростков в понимании родителей и учителей (Ч. 1. Постановка проблемы) [Электронный ресурс] // Психология и право. 2015. Том 5. № 3. С. 1—13. doi:10.17759/psylaw.2015050301
9. *Борисова Е.С., Белоусов А.Л.* Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы // Актуальные проблемы экономики и права. 2019. Том 13. № 3. С. 1330—1342. doi:10.21202/1993-047X.13.2019.3.1330-1342
10. *Будыкин С.В.* Информационная безопасность детей и подростков в современном мире: психологические аспекты проблемы // Юридическая психология. 2017. № 1. С. 13—24.

11. *Будыкин С.В., Дворянчиков Н.В., Бовина И.Б.* Информационная безопасность детей и подростков в представлениях родителей [Электронный ресурс] // Психологическая наука и образование. 2016. Том 8. № 4. С. 117—126. doi:10.17759/psyedu.2016080412
12. *Будыкин С.В., Дворянчиков Н.В., Бовина И.Б.* Информационная безопасность детей и подростков в понимании родителей и учителей (Ч. 2. Результаты эмпирического исследования) [Электронный ресурс] // Психология и право. 2016. Том 6. № 1. С. 25—38. doi:10.17759/psylaw.2016060104
13. *Будыкин С.В.* Информационная безопасность детей и подростков в современном мире: психологические аспекты проблемы [Электронный ресурс] // Психология и право. 2017. Том 7. № 1. С. 13—24. doi:10.17759/psylaw.2017070102
14. *Дворянчиков Н.В., Будыкин С.В., Пимонов В.А., Бовина И.Б.* Информационная безопасность детей и подростков: юридические и психологические аспекты проблемы // Юридическая психология. 2016. № 1. С. 31—35.
15. *Кузнецова Ю.М., Чудова Н.В.* Психология жителей Интернета. М.: Изд-во ЛКИ, 2008. 224 с.
16. *Кулемина А.Е.* Особенности формирования культуры информационной безопасности в федеральных органах государственной власти // Сборник трудов конференции молодых ученых. Вып. 6: Информационные технологии. СПб: СПбГУ ИТМО, 2009. 707 с.
17. *Манзи Д.С.* Управление рынком дезинформации: первая поправка и борьба против фейковых новостей // Актуальные проблемы экономики и права. 2020. Том 14. № 1. С. 141—163. doi:10.21202/1993-047X.14.2020.1.141-163
18. *Соколова М.В., Дозорцева Е.Г.* Склонность к аутоагрессивному поведению у подростков и информация, потребляемая ими в Интернете [Электронный ресурс] // Психология и право. 2019. Том 9. № 1. С. 22—35. doi:10.17759/psylaw.2019090102
19. *Чеботарева А.А.* Обеспечение информационной безопасности личности в Интернете: история и проблемы развития законодательства // История государства и права. 2010. № 11. С. 30—33.
20. *Шпагина Е.М., Чиркина Р.В.* Компетентность педагогов и психологов в области информационной безопасности детей [Электронный ресурс] // Психология и право. 2019. Том 9. № 3. С. 261—277. doi:10.17759/psylaw.2019090319
21. *Шпагина Е.М.* Информационная безопасность в контексте защиты прав детей в Российской Федерации [Электронный ресурс] // Психология и право. 2016. Том 6. № 4. С. 86—94. doi:10.17759/psylaw.2016060409.
22. *Ahmad Z., Ong T., Liew T., Norhashim M.* Security monitoring and information security assurance behaviour among employees: An empirical analysis // Information and Computer Security. 2019. Vol. 27. Iss. 2. P. 165—188. doi:10.1108/ICS-10-2017-0073
23. *Algarni M., Almesalm S., Syed M.* Towards Enhanced Comprehension of Human Errors in Cybersecurity Attacks // International Conference on Applied Human Factors and Ergonomics. Advances in Human Error, Reliability, Resilience, and Performance. 2018. Vol. 778. P. 163—175. doi:10.1007/978-3-319-94391-6_16
24. *Al Hogail A., Mirza A.* Information security culture: A definition and a literature review // World Congress on Computer Applications and Information Systems. 2014. P. 1—7. doi:10.1109/WCCAIS.2014.6916579

25. *Beena A.L., Dr. Humayoon Kabir S.* Information Security Insider Threats in Organizations and Mitigation Techniques // International Conference on Recent Advances in Energy-efficient Computing and Communication. 2019. P. 1—4. doi:10.1109/ICRAECC43874.2019.8995088
26. *Bovina I.B., Dvoryanchikov N.V., Budykin S.V.* Shared meaning about information security of children: an exploratory study // Procedia — Social and Behavioral Sciences. 2014. Vol. 146. P. 94—98.
27. *Corradini I., Nardelli E.* Building Organizational Risk Culture in Cyber Security: The Role of Human Factors // International Conference on Applied Human Factors and Ergonomics. Advances in Human Factors in Cybersecurity. 2019. Vol. 782. P. 193—202. doi:10.1007/978-3-319-94782-2_19
28. *Corradini I., Nardelli E.* Social Engineering and the Value of Data: The Need of Specific Awareness Programs // International Conference on Applied Human Factors and Ergonomics. Advances in Human Factors in Cybersecurity. 2020. Vol. 960. P. 59—65. doi:10.1007/978-3-030-20488-4_6
29. *Da Veiga A., Astakhova L.V., Botha A., Herselman M.* Defining organisational information security culture - Perspectives from academia and industry // Computers & Security. 2020. Vol. 92, art. 101713. doi:10.1016/j.cose.2020.101713
30. *Da Veiga A., Martins N.* Information security culture and information protection culture: A validated assessment instrument // Computer Law & Security Review. 2015. Vol. 31. Iss. 2. P. 243—256. doi:10.1016/j.clsr.2015.01.005
31. *Glaspie H.W., Karwowski W.* Human Factors in Information Security Culture: A Literature Review // International Conference on Applied Human Factors and Ergonomics. Advances in Human Factors in Cybersecurity. 2017. Vol. 593. P. 269—280. doi:10.1007/978-3-319-60585-2_25
32. *Halevi T., Memon N., Lewis J., Kumaraguru P., Arora S., Dagar N., Aloul F., Chen J.* Cultural and psychological factors in cyber-security // Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services. 2016. P. 318—324. doi:10.1145/3011141.3011165
33. *Kennedy S.E.* The pathway to security - mitigating user negligence // Information and Computer Security. 2016. Vol. 24. Iss. 3. P. 255—264. doi:10.1108/ICS-10-2014-0065
34. *Martins A., Elofe J.* Information Security Culture // Security in the Information Society. IFIP Advances in Information and Communication Technology. 2002. Vol. 86. P. 203—214. doi:10.1007/978-0-387-35586-3_46
35. *McCormac A., Zwaans T., Parsons K.M., Calic D., Butavicius M.A., Pattinson M.R.* Features of Manipulative Behavior in Operational Officers' Professional Activity // Computers in Human Behavior. 2017. Vol. 69. P. 151—156. doi:10.1016/j.chb.2016.11.065
36. *Nasir A., Abdullah Arshah R., Ab Hamid M.R., Fahmy S.* An analysis on the dimensions of information security culture concept: A review // Journal of Information Security and Applications. 2019. Vol. 44. P. 12—22. doi:10.1016/j.jisa.2018.11.003
37. *Okere I., Van Niekerk J.F., Carroll M.* Assessing information security culture: A critical analysis of current approaches // Information Security for South Africa. 2012. P. 1—8. doi:10.1109/ISSA.2012.6320442
38. *Parsons K.M., Young E., Butavicius M.A., McCormac A., Pattinson M.R., Jerram C.* The Influence of Organizational Information Security Culture on Information Security Decision Making // Journal of Cognitive Engineering and Decision Making. 2015. Vol. 9. Iss. 2. P. 117—129. doi:10.1177/1555343415575152

39. *Ramachandran S., Rao S.V., Goles T.* Information Security Cultures of Four Professions: A Comparative Study // Proceedings of the 41st Annual Hawaii International Conference on System Sciences. 2008. P. 454—454. doi:10.1109/HICSS.2008.201
40. *Schlienger T., Teufel S.* Information Security Culture. The Socio-Cultural Dimension in Information Security Management // Security in the Information Society. IFIP Advances in Information and Communication Technology. 2002. Vol. 86. P. 191—201. doi:10.1007/978-0-387-35586-3_46
41. *Tang M., Li M., Zhang T.* The impacts of organizational culture on information security culture: a case study // Information Technology and Management. 2016. Vol. 17. Iss. 2. P. 179—186. doi:10.1007/s10799-015-0252-2
42. *Thomson K., Van Niekerk J.F.* Combating information security apathy by encouraging prosocial organisational behavior // Information Management & Computer Security. 2012. Vol. 20. Iss. 1. P. 39—46. doi:10.1108/09685221211219191
43. *Van Niekerk J.F., Von Solms R.* Information security culture: A management perspective // Computers & Security. 2010. Vol. 29. Iss. 4. P. 476—486. doi:10.1016/j.cose.2009.10.005
44. *Wiley A., McCormac A., Calic D.* More than the individual: Examining the relationship between culture and Information Security Awareness // Computers & Security. 2020. Vol. 88, art. 101640. doi:10.1016/j.cose.2019.101640
45. *Zhumagaliyeva B., Barabanova E.* Features of Manipulative Behavior in Operational Officers' Professional Activity // Procedia — Social and Behavioral Sciences. 2017. Vol. 140. P. 9—14. doi:10.1016/j.sbspro.2014.04.379

References

1. Begishev I.R. Sindrom bezopasnoj ataki: juridiko-psihologicheskij fenomen [Safe attack syndrome: a legal and psychological phenomenon]. *Juridicheskaja psihologija [Legal psychology]*, 2018, no. 2, pp. 27—30. (In Russ., Abstr. in Engl.).
2. Begishev I.R., Khisamova Z.I., Nikitin S.G. Organizacija hakerskogo soobshhestva: kriminologicheskij i ugolovno-pravovoj aspekty [Organization of the hacker community: criminological and criminal-legal aspects]. *Vserossijskij kriminologicheskij zhurnal [Russian Journal of Criminology]*, 2020, Vol. 14, no. 1, pp. 96—105. doi:10.17150/2500-4255.2020.14(1).96-105 (In Russ., Abstr. in Engl.).
3. Begishev I.R., Bikeev I.I. Prestuplenija v sfere obrashhenija cifrovoj informacii [Crimes in the sphere of digital information circulation]. Kazan: Kazan Innovation University Publ., 2020. 300 p.
4. Bovina I.B., Dvoryanchikov N.V., Budykin S.V. Informacionnaja bezopasnost' detej v obydennom ponimanii roditelej i uchitelej [Information security of children in the everyday understanding of parents and teachers]. *Vestnik Rossijskogo universiteta druzhby narodov. Serija: Psihologija i pedagogika [Bulletin of the Russian University of peoples ' friendship. Series: Psychology and pedagogy]*, 2016, no. 1, pp. 77—86. (In Russ., Abstr. in Engl.).
5. Bovina I.B., et al. Social'nye predstavlenija i informacionnaja bezopasnost' detej i podrostkov: tochka zrenija uchitelej (Chast' 1) [Elektronnyi resurs] [Social representations and information security of children and adolescents: the point of view of teachers (Part 1)]. *Psikhologiia i pravo [Psychology and Law]*, 2017, Vol. 7, no. 1, pp. 1—12. doi:10.17759/psylaw.2017070101 (In Russ., Abstr. in Engl.).
6. Bovina I.B., et al. Social'nye predstavlenija i informacionnaja bezopasnost' detej i podrostkov: tochka zrenija uchitelej (Chast' 2) [Elektronnyi resurs] [Social representations and information

security of children and adolescents: the point of view of teachers (Part 2)]. *Psikhologiia i pravo [Psychology and Law]*, 2017, Vol. 7, no. 2, pp. 19—32. doi:10.17759/psylaw.2017060202 (In Russ., Abstr. in Engl.).
7. Bovina I.B., et al. Social'nye predstavlenija i informacionnaja bezopasnost' detej i podrostkov: tochka zrenija uchitelej (Chast' 3) [Elektronnyi resurs] [Social representations and information security of children and adolescents: the point of view of teachers (Part 3)]. *Psikhologiia i pravo [Psychology and Law]*, 2017, Vol. 7, no. 3, pp. 138—148. doi:10.17759/psylaw.2017070311 (In Russ., Abstr. in Engl.).
8. Bovina I.B., Dvoryanchikov N.V., Budykin S.V. Informacionnaja bezopasnost' detej i podrostkov v ponimanii roditelej i uchitelej (Ch. 1. Postanovka problemy) [Elektronnyi resurs] [Information security of children and adolescents in the understanding of parents and teachers (Part 1. Statement of the problem)]. *Psikhologiia i pravo [Psychology and Law]*, 2015, Vol. 5, no. 3, pp. 1—13. doi:10.17759/psylaw.2015050301 (In Russ., Abstr. in Engl.).
9. Borisova E.S., Belousov A.L. Innovacii kak instrument obespechenija informacionnoj bezopasnosti i povyshenija jeffektivnosti dejatel'nosti bankovskoj sistemy [Elektronnyi resurs] [Innovations as a tool for ensuring information security and improving the efficiency of the banking system]. *Aktual'nye problemy jekonomiki i prava [Actual Problems of Economics and Law]*, 2019, Vol. 13, no. 3, pp. 1330—1342. doi:10.21202/1993-047X.13.2019.3.1330-1342 (In Russ., Abstr. in Engl.).
10. Budykin S. V. Informacionnaja bezopasnost' detej i podrostkov v sovremennom mire: psihologicheskie aspekty problemy [Information security of children and adolescents in the modern world: psychological aspects of the problem]. *Juridicheskaja psihologija [Legal psychology]*, 2017, no. 1, pp. 13—24. (In Russ., Abstr. in Engl.).
11. Budykin S.V., Dvoryanchikov N.V., Bovina I.B. Informacionnaja bezopasnost' detej i podrostkov v predstavlenijah roditelej [Elektronnyi resurs] [Information security of children and adolescents in the representations of parents]. *Psihologicheskaja nauka i obrazovanie [Psychological science and education]*, 2016, Vol. 8, no. 4, pp. 117—126. doi:10.17759/psyedu.2016080412 (In Russ., Abstr. in Engl.).
12. Budykin S.V., Dvoryanchikov N.V., Bovina I.B. Informacionnaja bezopasnost' detej i podrostkov v ponimanii roditelej i uchitelej)] [Elektronnyi resurs] (Ch. 2. Rezul'taty jempiricheskogo issledovanija) [Information security of children and adolescents in the understanding of parents and teachers (Part 2. Results of empirical research. *Psikhologiia i pravo [Psychology and Law]*, 2016, Vol. 6, no. 1, pp. 25—38. doi:10.17759/psylaw.2016060104 (In Russ., Abstr. in Engl.).
13. Budykin S.V. Informacionnaja bezopasnost' detej i podrostkov v sovremennom mire: psihologicheskie aspekty problemy [Elektronnyi resurs] [Information security of children and adolescents in the modern world: psychological aspects of the problem]. *Psikhologiia i pravo [Psychology and Law]*, 2017, Vol. 7, no. 1, pp. 13—24. doi:10.17759/psylaw.2017070102 (In Russ., Abstr. in Engl.).
14. Dvoryanchikov N.V., et al. Informacionnaja bezopasnost' detej i podrostkov: juridicheskie i psihologicheskie aspekty problemy [Information security of children and adolescents: legal and psychological aspects of the problem]. *Juridicheskaja psihologija [Legal psychology]*, 2016, no. 1, pp. 31—35. (In Russ., Abstr. in Engl.).
15. Kuznetsova Yu.M., Chudova N.V. Psihologija zhitelej Interneta [Psychology of Internet users]. Moscow: LKI Publ., 2008. 224 p.

16. Kulemina A.E. Osobennosti formirovanija kul'tury informacionnoj bezopasnosti v federal'nyh organah gosudarstvennoj vlasti [Features of formation of information security culture in Federal state authorities]. In. *Proceedings of the conference of young scientists*, vol. 6, Information technology. Saint-Petersburg: ITMO University Publ., 2009. 707 p.
17. Manzi D.S. Upravlenie rynkom dezinformacii: pervaja popravka i bor'ba protiv fejkovyh novostej [Managing the disinformation market: the first amendment and the fight against fake news]. *Aktual'nye problemy jekonomiki i prava [Actual Problems of Economics and Law]*, 2020, Vol. 14, no. 1, pp. 141—163. doi:10.21202/1993-047X.14.2020.1.141-163 (In Russ., Abstr. in Engl.).
18. Sokolova M.V., Dozortseva E.G. Sklonnost' k autoagressivnomu povedeniju u podrostkov i informacija, potrebljaemaja imi v Internete [Elektronnyi resurs] [Propensity to autoagressive behavior in adolescents and information consumed by them on the Internet]. *Psikhologiia i pravo [Psychology and Law]*, 2019, Vol. 9, no. 1, pp. 22—35. doi:10.17759/psylaw.2019090102 (In Russ., Abstr. in Engl.).
19. Chebotareva A.A. Obespechenie informacionnoj bezopasnosti lichnosti v Internete: istorija i problemy razvitija zakonodatel'stva [Ensuring information security of the individual on the Internet: history and problems of legislation development]. *Istorija gosudarstva i prava [History of the state and law]*, 2010, no. 11, pp. 30—33. (In Russ., Abstr. in Engl.).
20. Shpagina E.M., Chirkina R.V. Kompetentnost' pedagogov i psihologov v oblasti informacionnoj bezopasnosti detej [Elektronnyi resurs] [Competence of teachers and psychologists in the field of information security of children]. *Psikhologiia i pravo [Psychology and Law]*, 2019, Vol. 9, no. 3, pp. 261—277. doi:10.17759/psylaw.2019090319 (In Russ., Abstr. in Engl.).
21. Shpagina E.M. Informacionnaja bezopasnost' v kontekste zashhity prav detej v Rossijskoj Federacii [Elektronnyi resurs] [Information security in the context of protection of children's rights in the Russian Federation]. *Psikhologiia i pravo [Psychology and Law]*, 2016, Vol. 6, no. 4, pp. 86—94. doi:10.17759/psylaw.2016060409 (In Russ., Abstr. in Engl.).
22. Ahmad Z., et al. Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information and Computer Security*, 2019, Vol. 27, no. 2, pp. 165—188. doi:10.1108/ICS-10-2017-0073
23. Algarni M., Almesalm S., Syed M. Towards Enhanced Comprehension of Human Errors in Cybersecurity Attacks. *International Conference on Applied Human Factors and Ergonomics. Advances in Human Error, Reliability, Resilience, and Performance*, 2018, Vol. 778, pp. 163—175. doi:10.1007/978-3-319-94391-6_16
24. Al Hogail A., Mirza A. Information security culture: A definition and a literature review. *World Congress on Computer Applications and Information Systems*, 2014, pp. 1—7. doi:10.1109/WCCAIS.2014.6916579
25. Beena A.L., Dr. Humayoon Kabir S. Information Security Insider Threats in Organizations and Mitigation Techniques. *International Conference on Recent Advances in Energy-efficient Computing and Communication*, 2019, pp. 1—4. doi:10.1109/ICRAECC43874.2019.8995088
26. Bovina I.B., Dvoryanchikov N.V., Budykin S.V. Shared meaning about information security of children: an exploratory study. *Procedia - Social and Behavioral Sciences*, 2014, Vol. 146, pp. 94—98.
27. Corradini I., Nardelli E. Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. *International Conference on Applied Human Factors and Ergonomics. Advances in*

Human Factors in Cybersecurity, 2019, Vol. 782, pp. 193—202. doi:10.1007/978-3-319-94782-2_19
28. Corradini I., Nardelli E. Social Engineering and the Value of Data: The Need of Specific Awareness Programs. *International Conference on Applied Human Factors and Ergonomics. Advances in Human Factors in Cybersecurity*, 2020, Vol. 960, pp. 59—65. doi:10.1007/978-3-030-20488-4_6
29. Da Veiga A., et al. Defining organisational information security culture — Perspectives from academia and industry. *Computers & Security*, 2020, Vol. 92, art. 101713. doi:10.1016/j.cose.2020.101713
30. Da Veiga A., Martins N. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 2015, Vol. 31, iss. 2, pp. 243—256. doi:10.1016/j.clsr.2015.01.005
31. Glaspie H.W., Karwowski W. Human Factors in Information Security Culture: A Literature Review. *International Conference on Applied Human Factors and Ergonomics. Advances in Human Factors in Cybersecurity*, 2017, Vol. 593, pp. 269—280. doi:10.1007/978-3-319-60585-2_25
32. Halevi T., et al. Cultural and psychological factors in cyber-security. *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services*, 2016, pp. 318—324. doi:10.1145/3011141.3011165
33. Kennedy S.E. The pathway to security - mitigating user negligence. *Information and Computer Security*, 2016, Vol. 24, iss. 3, pp. 255—264. doi:10.1108/ICS-10-2014-0065
34. Martins A., Elofe J. Information Security Culture. *Security in the Information Society. IFIP Advances in Information and Communication Technology*, 2002, Vol. 86, pp. 203—214. doi:10.1007/978-0-387-35586-3_46
35. McCormac A., et al. Features of Manipulative Behavior in Operational Officers' Professional Activity. *Computers in Human Behavior*, 2017, Vol. 69, pp. 151—156. doi:10.1016/j.chb.2016.11.065
36. Nasir A., et al. An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, 2019, Vol. 44, pp. 12—22. doi:10.1016/j.jisa.2018.11.003
37. Okere I., Van Niekerk J.F., Carroll M. Assessing information security culture: A critical analysis of current approaches. *Information Security for South Africa*, 2012, pp. 1—8. doi:10.1109/ISSA.2012.6320442
38. Parsons K.M., et al. The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, 2015, Vol. 9, no. 2, pp. 117—129. doi:10.1177/1555343415575152
39. Ramachandran S., Rao S.V., Goles T. Information Security Cultures of Four Professions: A Comparative Study. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, 2008, pp. 454—454. doi:10.1109/HICSS.2008.201
40. Schlienger T., Teufel S. Information Security Culture. The Socio-Cultural Dimension in Information Security Management. *Security in the Information Society. IFIP Advances in Information and Communication Technology*, 2002, Vol. 86, pp. 191—201. doi:10.1007/978-0-387-35586-3_46

41. Tang M., Li M., Zhang T. The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 2016, Vol. 17, no. 2, pp. 179—186. doi:10.1007/s10799-015-0252-2
42. Thomson K., Van Niekerk J.F. Combating information security apathy by encouraging prosocial organisational behavior. *Information Management & Computer Security*, 2012, Vol. 20, no. 1, pp. 39—46. doi:10.1108/09685221211219191
43. Van Niekerk J.F., Von Solms R. Information security culture: A management perspective. *Computers & Security*, 2010, Vol. 29, no. 4, pp. 476—486. doi:10.1016/j.cose.2009.10.005
44. Wiley A., McCormac A., Calic D. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 2020, Vol. 88, art. 101640. doi:10.1016/j.cose.2019.101640
45. Zhumagaliyeva B., Barabanova E. Features of Manipulative Behavior in Operational Officers' Professional Activity. *Procedia — Social and Behavioral Sciences*, 2017, Vol. 140, pp. 9—14. doi:10.1016/j.sbspro.2014.04.379

Информация об авторах

Бегишев Ильдар Рустамович, кандидат юридических наук, заслуженный юрист Республики Татарстан, старший научный сотрудник, Казанский инновационный университет имени В.Г. Тимирясова (КИУ им. В.Г. Тимирясова), г. Казань, Российская Федерация, ORCID: https://orcid.org/0000-0001-5619-4025, e-mail: begishev@mail.ru

Information about the authors

Ildar R. Begishev, PhD in Law, Honored Lawyer of the Republic of Tatarstan, Senior Researcher, Kazan Innovative University named after V.G. Timiryasov, Kazan, Russian Federation, ORCID: https://orcid.org/0000-0001-5619-4025, e-mail: begishev@mail.ru

Получена 13.03.2020
Принята в печать 10.11.2021

Received 13.03.2020
Accepted 10.11.2021