
ЦИФРОВАЯ СРЕДА

Влияние цифровой среды, интернет-зависимости и цифровой тревожности на культуру информационной безопасности у менеджеров поколения Z

УДК 316.6

DOI 10.26425/2658-347X-2025-8-3-34-43

Получено: 25.07.2025

Доработано после рецензирования: 11.09.2025

Принято: 18.09.2025

Гасанова Земфира Бейдуллаховна

Канд. пед. наук, доц. каф. политического анализа
и социально-психологических процессов

ORCID: 0009-0000-2273-031X

E-mail: gasanova.zb@rea.ru

Российский экономический университет им. Г.В. Плеханова,
г. Москва, Россия

Гасанов Магомедали Изафидинович

Студент

ORCID: 0009-0003-6688-0426

E-mail: texnichno1337@gmail.com

Российский экономический университет им. Г.В. Плеханова,
г. Москва, Россия

АННОТАЦИЯ

Изучена культура информационной безопасности как системный феномен, определяющий поведение менеджеров поколения Z в цифровой среде. Интернет-зависимость и цифровая тревожность выступают социально-психологическими факторами, влияющими на индивидуальные привычки цифровой гигиены и соблюдение правил информационной безопасности. Раскрыт психологический портрет менеджеров поколения Z, чем они отличаются от других поколений и какие в связи с этим возникают социально-психологические проблемы. Особое внимание уделено новым социальным явлениям, ставшими массовыми, таким как появление интернет-зависимости и цифровой тревожности у менеджеров поколения Z, дано объяснение этих научных терминов и того, каким образом они влияют на культуру информационной безопасности. Описаны структурные компоненты культуры информационной безопасности (ценности и нормы, знания и навыки, повседневные практики, лидерство и организационные артефакты) и их связь

с управленческой деятельностью менеджеров. Проведен анализ того, к каким негативным последствиям в контексте управленческой деятельности цифровая тревожность, интернет-зависимость и несоблюдение цифровой гигиены могут привести на уровне организации и личности в целом. Для профилактики и коррекции интернет-зависимости и цифровой тревожности менеджеров поколения Z в контексте цифровой гигиены и информационной безопасности предложен комплексный подход решения данной научной проблемы, включающий как индивидуальные психологические стратегии (цифровой детокс, когнитивно-поведенческие техники, развитие офлайн-активностей и социальных связей, цифровой гигиены менеджера и усиление информационной безопасности, практики осознанности и внимательности), так и организационные стратегии (создание культуры информационной безопасности и цифрового благополучия, пересмотр метрик эффективности, поддержка баланса работы и личной жизни).

Ключевые слова

Цифровая среда, культура информационной безопасности, социально-психологические факторы, интернет-зависимость, цифровая тревожность, менеджеры поколения Z, цифровая гигиена, цифровое благополучие

Для цитирования

Гасанова З.Б., Гасанов М.И. Влияние цифровой среды, интернет-зависимости и цифровой тревожности на культуру информационной безопасности у менеджеров поколения Z // Цифровая социология. 2025. Т. 8. № 3. С. 34–43.

© Гасанова З.Б., Гасанов М.И., 2025.

Статья доступна по лицензии Creative Commons "Attribution" («Атрибуция») 4.0. всемирная (<http://creativecommons.org/licenses/by/4.0/>).



DIGITAL ENVIRONMENT

The impact of digital environment, internet addiction, and digital anxiety on information security culture among generation Z managers

Received 25.07.2025

Revised 11.09.2025

Accepted 18.09.2025

Zemfira B. Gasanova

Cand. Sci. (Ped.), Assoc. Prof. at the Political Analysis and Socio-Psychological Processes Department

ORCID: 0009-0000-2273-031X

E-mail: gasanova.zb@rea.ru

Plekhanov Russian University of Economics, Moscow, Russia

Magomedali I. Gasanov

Student

ORCID: 0009-0003-6688-0426

E-mail: texnichno1337@gmail.com

Plekhanov Russian University of Economics, Moscow, Russia

ABSTRACT

Information security culture has been studied as a systemic phenomenon that determines generation Z managers' behavior in the digital environment. Internet addiction and digital anxiety are socio-psychological factors affecting individual digital hygiene habits and compliance with information security rules. The psychological portrait of generation Z managers has been revealed, how they differ from other generations, and what socio-psychological problems arise in this regard. Special attention has been paid to new social phenomena that have become widespread, such as the emergence of Internet addiction and digital anxiety among generation Z managers, and an explanation of these scientific terms and how they affect information security culture has been given. The structural components of information security culture (values and norms, knowledge and skills, daily practices, leadership, and organizational artifacts) and their relationship to management activities of generation

Z people have been described. The analysis of what negative consequences in the context of management activities digital anxiety, Internet addiction, and digital hygiene non-observance can lead to at the level of an organization and personality as a whole has been carried out. For preventing and correcting Internet addiction and digital anxiety in generation Z managers in the context of digital hygiene and information security, a comprehensive approach to solving this scientific issue has been proposed, including both individual psychological strategies (digital detox, cognitive behavioral techniques, development of offline activities and social connections, manager's digital hygiene, strengthening information security, and mindfulness practices), as well as organizational strategies (creating a culture of information security and digital well-being, reviewing performance metrics, and maintaining work-life balance).

Keywords

Digital environment, information security culture, socio-psychological factors, Internet addiction, digital anxiety, generation Z managers, digital hygiene, digital well-being

For citation

Gasanova Z.B., Gasanov M.I. (2025) The impact of digital environment, internet addiction, and digital anxiety on information security culture among generation Z managers. *Digital sociology*. Vol. 8, no 3, pp. 34–43. DOI: 10.26425/2658-347X-2025-8-3-34-43



ВВЕДЕНИЕ / INTRODUCTION

В современном мире цифровых инноваций сеть «Интернет» (далее – Интернет) стала важной частью человеческих реалий, особенно у зумеров (поколение Z), родившихся примерно с середины 1990-х гг. по начало 2010-х гг., которые выросли в то время, когда цифровые технологии стали нормой обычной жизни. Их характеризуют высокая цифровая грамотность, стремление к индивидуальности и свободе, а также практичность и ориентация на «здесь и сейчас». С воздействием информационной среды мы связываем свойственные поколению Z прагматизм, стремление к выбору наиболее эффективного решения, умение за краткое время находить нужную информацию, позволяющую повысить объективность восприятия [Бреслер, Алексеева, 2024].

В данной статье культура информационной безопасности выступает основой для анализа.

Цель настоящего исследования – проанализировать влияние цифровой среды, интернет-зависимости и цифровой тревожности на культуру информационной безопасности у менеджеров поколения Z. Мы рассмотрим интернет-зависимость и цифровую тревожность как взаимосвязанные социально-психологические феномены, которые модифицируют отношение зумеров-менеджеров к рискам, правилам, цифровой гигиене и, следовательно, соблюдению информационной безопасности, а также как особенности когнитивной архитектуры «всегда онлайн», ценности гибкости и скорости и давление «оперативности ответа» отражаются на повседневных управленческих практиках и создают новые уязвимости и как эти уязвимости можно компенсировать средствами культуры информационной безопасности.

Поколение Z часто называют «цифровыми аборигенами», поскольку его представители с раннего детства погружены в цифровую среду. Это поколение отличается высокой скоростью обработки информации, многозадачностью и предпочтением визуального контента.

Процесс цифровизации неизбежно меняет структуру занятости населения и образовательную среду как поставщика кадров, которые будут работать в совершенно иных по сравнению с прежними условиях [Гасанова, Пожарская, 2022]. Для менеджеров поколения Z, выросших в цифровой среде и постоянной сетевой вовлеченности, культура информационной безопасности одновременно является вызовом и конкурентным преимуществом. Она соотносится с задачами национальной и информационно-психологической безопасности. По мере того, как представите-

ли этого поколения вступают в управленческие роли, возникают новые социально-психологические явления, требующие научного осмысления. Среди них особое место занимают проблемы интернет-зависимости и цифровой тревожности и их отношения к информационной безопасности, что влияет на устойчивость организаций и социума в целом.

В условиях трансформации общеполитических и социально-экономических процессов управление и подготовка высококвалифицированных кадров, обладающих цифровыми компетенциями, является доминирующим фактором развития и благополучия страны, значимости в международном мире, основой национальной безопасности [Гасанова, Гасанов, 2024]. С психологической точки зрения постоянное взаимодействие с цифровыми технологиями формирует особую когнитивную архитектуру. Исследования Б. Спарроу и коллег показали, что интенсивное использование Интернета меняет способы запоминания информации: вместо самого содержания люди запоминают путь доступа к нему [Sparrow, Liu, Wegner, 2011].

Находим справедливым высказывание Т.М. Краснянской, В.Г. Тылец, В.В. Иохвидова о том, что развитие предметного поля информационно-психологической безопасности образуется двумя основными блоками вопросов, касающихся природы информационного воздействия на психику человека и связанных с психологическими эффектами информационных воздействий на него. Первый блок помещает проблематику информационно-психологической безопасности в поле интересов технических наук, разрабатывающих теорию информации, второй – в поле интересов психологической науки [Краснянская, Тылец, Иохвидов, 2021]. Таким образом, Интернет становится своеобразным «внешним жестким диском» для когнитивной системы человека.

Вхождение представителей поколения Z в управленческие позиции характеризуется рядом особенностей. Согласно данным Deloitte (2022), к 2025 г. поколение Z будет составлять около 27 % рабочей силы в корпоративном секторе, а 15 % из них займут позиции младшего и среднего менеджмента. Исследования показали, что менеджеры поколения Z демонстрируют следующие характеристики:

- предпочтение цифровых каналов коммуникации;
- высокая ценность информационной безопасности графика и удаленной работы;
- стремление к быстрому принятию решений на основе данных;
- ориентацию на социально ответственный бизнес.

Однако, как отмечают Дж. М. Твенге и У.К. Кемпбелл, постоянное пребывание в цифровой среде создает предпосылки для развития интернет-зависимости и связанных с ней социально-психологических проблем, включая цифровую тревожность, которые могут существенно влиять на управленческие компетенции и цифровую безопасность [Twenge, Campbell, 2019]. Таким образом, цифровизация в современных научных исследованиях нередко рассматривается в качестве созидательной силы, порождающей новые цифровые технологии, целевое использование которых может носить как конструктивный, так и деструктивный характер [Щербакова, Осипов, 2025].

КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОНЯТИЕ, СТРУКТУРА, РОЛЬ МЕНЕДЖЕРА ПОКОЛЕНИЯ Z / INFORMATION SECURITY CULTURE: CONCEPT, STRUCTURE, A GENERATION Z MANAGER ROLE

Под культурой информационной безопасности мы понимаем совокупность разделяемых в организации представлений о ценности информации, норм и правил ее защиты, устойчивых практик и артефактов (политик, процессов, инструментов), а также образцов лидерского поведения, подкрепляющих безопасные решения в повседневной работе. Культура информационной безопасности – это комплекс знаний, навыков, ценностей и норм поведения, который обеспечивает безопасное взаимодействие человека с информацией в цифровом пространстве, а также устойчивую защиту данных в организации. Она включает понимание угроз, соблюдение правил и политик безопасности, а также осознанное и ответственное поведение сотрудников при работе с конфиденциальной информацией, что является ключевым фактором устойчивости систем защиты.

Для менеджеров поколения Z критичны четыре взаимосвязанных уровня:

- ценности и нормы – «безопасность по умолчанию» как ценность, совместимая с ориентацией на скорость и инновации, нормативные ожидания по конфиденциальности и этике данных;
- знания и навыки – фундамент цифровой грамотности: модели угроз, фишинг и социальная инженерия, управление доступами, приватность по умолчанию, защита персональных устройств;
- практики и рутины – ежедневные привычки цифровой гигиены: многофакторная аутентификация, менеджеры паролей, обновления, «чистые» рабочие пространства и экраны, минимизация «шэринга» (экономическая модель, основанная на совместном использовании ресурсов,

товаров или услуг между людьми через специальные платформы) и принцип наименьших привилегий;

- лидерство и артефакты – ролевые модели, простые и ясные политики, «безопасные» интерфейсы и настройки по умолчанию, обучающие симуляции, позитивное подкрепление безопасного поведения.

Именно менеджер среднего звена задает тон: он переводит политики в действующие правила команды, делает безопасность видимой и совместимой с бизнес-целями, управляет компромиссами «скорость ↔ надежность», распределяет внимание и ресурсы. Для поколения Z эта роль естественна благодаря цифровой компетентности, но осложняется рисками «переподключения» и высокой толерантностью к обмену данными.

ИНТЕРНЕТ-ЗАВИСИМОСТЬ КАК ВЫЗОВ КУЛЬТУРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ / INTERNET ADDICTION AS A CHALLENGE TO INFORMATION SECURITY CULTURE

Интернет-зависимость как социально-психологический феномен была впервые описана К. Янг в 1996 г. Интернет-зависимость определяют как компульсивное использование Интернета, которое приводит к нарушению психологического благополучия, социальных отношений и повседневного функционирования. С точки зрения современной клинической психологии, хотя она не имеет официального статуса отдельного расстройства в диагностических руководствах DSM-5 и МКБ-11, многие исследователи рассматривают ее как форму поведенческой зависимости.

Согласно модели Гриффитса, интернет-зависимость характеризуется 6 ключевыми компонентами [Griffiths, 2005]:

- сверхценность – Интернет становится доминирующей деятельностью в жизни человека;
- изменение настроения – использование Интернета для регуляции эмоционального состояния;
- толерантность – необходимость увеличивать время пребывания онлайн;
- симптомы отмены – психологический дискомфорт при отсутствии доступа к Интернету;
- конфликт – межличностные и внутриличностные проблемы, вызванные чрезмерным использованием Интернета;
- рецидив – тенденция к возврату к прежним паттернам использования после периодов контроля.

Исследования показывают, что распространенность интернет-зависимости среди представителей поколения Z составляет от 10 до 30 %

в зависимости от страны и используемых диагностических критериев. При этом наблюдаются значимые различия в паттернах зависимости: молодые мужчины чаще демонстрируют зависимость от онлайн-игр и порнографии, в то время как молодые женщины более склонны к зависимости от социальных сетей и онлайн-шоппинга [Cheng, Li, 2014].

С нейропсихологической точки зрения интернет-зависимость связана с изменениями в дофаминергической системе вознаграждения. Исследования с использованием функциональной магнитно-резонансной томографии (фМРТ) показывают, что у людей с интернет-зависимостью наблюдаются структурные и функциональные изменения в областях мозга, ответственных за самоконтроль, принятие решений и обработку эмоций, включая префронтальную кору и переднюю поясную кору.

В управленческом контексте она проявляется как:

- компульсивная проверка почты/мессенджеров и КРП;
- нескончаемая «онлайн-смена» без восстановления;
- постоянное стремление «быть в курсе» и демонстрировать отклик.

Связи с культурой информационной безопасности:

- повышенная импульсивность → поспешные клики по ссылкам и вложениям, игнорирование «красных флажков» фишинга;
- толерантность к риску утечки → повторное использование паролей, перенос рабочих файлов в личные облака «для удобства»;
- конфликт и выгорание → снижение внимательности к процедурам информационной безопасности и рост ошибок.

Эти паттерны поведения создают предпосылки для развития цифровой тревожности, которая может значительно снижать качество жизни и профессиональную эффективность. Следовательно, профилактика интернет-зависимости – это не только забота о благополучии, но и инструмент зрелости культуры информационной безопасности.

ЦИФРОВАЯ ТРЕВОЖНОСТЬ: ФЕНОМЕНОЛОГИЯ И ВЛИЯНИЕ НА БЕЗОПАСНОЕ ПОВЕДЕНИЕ / DIGITAL ANXIETY: PHENOMENOLOGY AND IMPACT ON SAFE BEHAVIOR

Цифровая тревожность представляет собой относительно новый психологический феномен, который привлекает все большее внимание исследователей. Согласно определению Рейденбер-

га и коллег, цифровая тревожность – это «состояние психологического дискомфорта, связанное с актуальным или ожидаемым взаимодействием с цифровыми технологиями или с отсутствием такого взаимодействия» [Reidenberg, Russell, Halevy, 2015].

В современной психологической литературе выделяют несколько типов цифровой тревожности:

- номофобия (англ. no-mobile-phone phobia) – страх остаться без мобильного телефона или доступа к Интернету;
- FoMO (Fear of Missing Out) – страх упустить важную информацию или социальные события;
- техностресс – тревога, связанная с необходимостью осваивать новые технологии и соответствовать темпу их развития;
- информационная перегрузка – тревога, вызванная избытком информации и необходимостью ее фильтрации;
- информационной безопасности ерхондрия – тревожное состояние, вызванное самодиагностикой на основе поиска медицинской информации в Интернете.

Исследования показывают, что распространенность различных форм цифровой тревожности среди представителей поколения Z достигает 45–60 % [Cheever, Rosen, Carrier, Chavez, 2014]. При этом у менеджеров этого поколения цифровая тревожность проявляется с особой интенсивностью из-за сочетания личной и профессиональной зависимости от цифровых технологий.

С психофизиологической точки зрения цифровая тревожность сопровождается классическими симптомами тревожных состояний: повышением уровня кортизола, учащением сердцебиения, мышечным напряжением, нарушениями сна. При этом существуют и специфические поведенческие проявления:

- компульсивная проверка устройств и уведомлений;
- ощущение «фантомной информационной безопасности рации» – ложное ощущение информационной безопасности рации телефона;
- избегание ситуаций с отсутствием доступа к Интернету;
- чрезмерная обеспокоенность онлайн-репутацией.

Для молодых менеджеров она усиливается рабочим теледавлением (англ. pressure to respond ASAP), что ухудшает восстановление и качество решений [Barber, Santuzzi, 2017].

Типичные эффекты для информационной безопасности:

- «поспешность любой ценой» – предпочтение скорости ответов процедурам проверки;

- «гипервнимание к шуму» – рост ложных тревог и снижение чувствительности к реальным угрозам;

- «избегание сложных правил» – обход политики информационной безопасности ради снижения тревоги и экономии времени.

В контексте управленческой деятельности цифровая тревожность может приводить к следующим негативным последствиям:

- снижение концентрации внимания и качества принимаемых решений;
- затруднения в установлении глубоких межличностных отношений с сотрудниками;
- размывание границ между работой и личной жизнью;
- повышенный риск эмоционального выгорания;
- снижение творческого потенциала из-за информационной перегрузки.

По данным исследования Salesforce (2023), 67 % молодых менеджеров испытывают симптомы цифровой тревожности не реже одного раза в неделю, а 42 % отмечают, что это состояние негативно влияет на их управленческую эффективность. Управленческие практики, поддерживающие культуру информационной безопасности, должны снижать тревожность: четкие ожидания доступности, предсказуемые окна ответа, разграничение каналов «срочно/не срочно», автоматические «тихие часы» и фокус-режимы.

Психологические факторы формирования культуры информационной безопасности у зумеров-менеджеров:

1) постоянная подключенность и многозадачность – представители поколения Z (зумеры) выросли в цифровой среде, не представляя мир без Интернета, что формирует у них потребность в постоянной подключенности и способности быстро переключаться между множеством цифровых задач и может приводить к:

- цифровой зависимости – невозможность отключиться от сети, постоянное желание проверить уведомления и быть в курсе событий может перерасти в аддикцию;

- цифровой тревоге – страх пропустить что-то важное (FoMO), необходимость быть всегда «на связи» и «в теме» порождают тревогу и напряжение;

2) формирование идентичности в цифровой среде – социальные сети и онлайн-платформы играют ключевую роль в самопрезентации и формировании идентичности для зумеров, что может сказаться на их тревожности.

Психологические особенности менеджеров поколения Z также влияют на их отношение к ин-

формационной безопасности, например, привычка к «открытости» и желание делиться информацией онлайн снижают бдительность в отношении конфиденциальности и защиты личных данных, а поверхностное понимание угроз информационной безопасности, таких как кибербуллинг, фишинг или утечки данных, может делать их более уязвимыми. Важно развивать навыки цифровой гигиены, цифровой грамотности и осознанности для защиты себя и своей организации от потенциальных рисков и формировать ответственное и осознанное отношение к своим действиям в сети и управлению информацией, а также найти баланс между использованием цифровых технологий для работы и жизни.

РЕКОМЕНДАЦИИ / RECOMMENDATIONS

Для избавления от негативных влияний интернет-зависимости и цифровой тревожности необходимо использовать комплексный подход, который включает индивидуальные психологические стратегии и организационные меры. Баланс достигается через конкретные регламенты и навыки. Ниже перечислены практики, которые показали устойчивый эффект в управленческой повседневности.

1. Индивидуальные стратегии. Для менеджеров поколения Z рекомендуются:

1) «окна без экрана» – 25–45 минут концентрированной работы с полностью отключенными уведомлениями, риск: импульсивные клики → снижается;

- внедрение практики «цифровых выходных» – периодов полного отключения от рабочих коммуникаций;

- использование техники «временных блоков» (англ. time-blocking) для фокусированной работы без отвлечений на цифровые устройства;

- установка четких границ между рабочим и личным временем с использованием настроек «Не беспокоить»;

2) когнитивно-поведенческие техники – метаанализ, проведенный Чан и коллегами, показал эффективность когнитивно-поведенческой терапии в снижении симптомов интернет-зависимости и связанной с ней тревожности [Chun, Shim, Kim, 2017]:

- мониторинг триггеров, вызывающих импульсивное использование Интернета;

- реструктуризация дисфункциональных убеждений (например, «Я должен немедленно отвечать на все сообщения»);

- разработка альтернативных способов удовлетворения психологических потребностей, ле-

жащих в основе зависимости;

3) практики осознанности и внимательности – растущий объем исследований подтверждает эффективность майндфулнесс-практик в снижении технологической зависимости и тревожности [Elhai, Dvorak, Levine, Hall, 2017]:

- регулярные медитативные практики, направленные на развитие способности находиться в настоящем моменте;

- техники «осознанного использования технологий», предполагающие внимательное отношение к цели и процессу взаимодействия с цифровыми устройствами;

- интеграция коротких практик осознанности в рабочий день (например, пятиминутные сессии внимательного дыхания между встречами);

4) развитие офлайн-активностей и социальных связей – исследования показывают, что расширение репертуара офлайн-занятий снижает риск интернет-зависимости и цифровой тревожности [Twenge, Campbell, 2019]:

- регулярная физическая активность;

- развитие глубоких личных отношений вне цифровой среды;

- хобби, не связанные с использованием цифровых технологий.

2. Организационные стратегии. Для менеджеров поколения Z рекомендуются:

1) «тихие часы» – в мессенджерах и почте по умолчанию 20:00–08:00 без уведомлений, исключения – только по роли, метрика: доля сотрудников с активным режимом «Не беспокоить»;

2) короткие симуляции фишинга – раз в месяц, 15–20 минут, кейсы собраны из реальной переписки отдела, метрика: доля распознанных писем, время реакции;

3) матрица доступов «минимально необходимый» – ежеквартальный пересмотр ролей, автоматический отзыв при уходе/смене должности, метрика: число лишних прав по итогам ревизии;

4) один понятный регламент – документ «Как мы работаем с данными» на две–три страницы: где хранить, как делиться, что делать при инциденте (контакты, сроки), метрика: доля сотрудников, прошедших ознакомление с контрольными вопросами;

5) MFA и парольная политика – обязательная 2FA для критичных систем, менеджер паролей рекомендован по умолчанию, необходимо разработать четкие и понятные политики, процедуры и стандарты безопасности, чтобы они соответствовали ценностям поколения Z, ограничивали ожидания по поводу доступности сотрудников во вне рабочее время и поощряли регулярные перерывы от экранов и цифровых ком-

муникаций, проводить тренинги по цифровому благополучию для менеджеров и сотрудников, а предоставление регулярной обратной связи и поддержки поможет сотрудникам развиваться и лучше справляться с вызовами в области безопасности, метрика: доля включенной MFA, причем культуру безопасности можно внедрять через:

- процедуры – короткий регламент + ролевые «шпаргалки» на страницу для руководителя, аналитика, HR;

- рутину – квартальные 15-минутные микро-курсы и разбор свежих кейсов из отдела вместо годового «большого» обучения;

- метрики поведения – не «Пройден курс», а MFA-покрытие, доля распознанных фишингов, время отзыва доступа;

- обратную связь – публичная разборка двух инцидентов/квазиинцидентов в месяц без персональных обвинений – что сработало, что не сработало в процессе;

6) пересмотр метрик эффективности – исследования показывают, что традиционные метрики, основанные на времени отклика и постоянной доступности, усиливают цифровую тревожность, при этом организации могут внедрять политики отключения рабочих коммуникаций во вне рабочее время, поощрять использование отпусков и дней отдыха без проверки рабочей почты, создавать культуру, где уважается право сотрудника на «цифровую паузу» [Barber, Santuzzi, 2017]:

- внедрение метрик, ориентированных на результат, а не на процесс и время отклика;

- отказ от культуры «всегда на связи» в пользу «значимой доступности»;

- оценка качества коммуникации, а не ее количества;

- поддержка баланса работы и личной жизни – согласно исследованиям, четкие границы между работой и личной жизнью способствуют психологическому благополучию и снижают риск цифровой зависимости [Sonnentag, Fritz, 2015];

7) специализированная поддержка для менеджеров поколения Z – учитывая специфические потребности этой группы, организации могут:

- разрабатывать программы менторинга, включающие аспекты цифрового благополучия;

- проводить регулярные интервизии и супервизии для обсуждения проблем цифрового стресса;

- предоставлять доступ к профессиональной психологической поддержке для преодоления цифровой зависимости и тревожности.

Как справедливо отмечает М. Михеева, рассматривая угрозы информационно-психологи-

ческой безопасности в контексте бизнес-среды, на менеджера высшего звена в высокой степени воздействуют как внешние факторы (бизнес-процессы в компании, отрасли, экономике, в мире, объем и масштаб информационных процессов), так и внутренние сложности (особенности переживания угроз на эмоционально-чувственном, интеллектуальном, мотивационном уровне) [Михеева, 2021]. Таким образом, мы приходим к выводу о том, что комплексный подход, сочетающий индивидуальные и организационные стратегии, наиболее эффективен в преодолении проблем интернет-зависимости и цифровой тревожности. Особенно важно учитывать индивидуальные особенности менеджеров поколения Z, включая их предыдущий опыт использования технологий, личностные черты и специфические профессиональные требования.

Интеграционная модель «информационная безопасность ↔ культура ↔ психология ↔ результат» состоит в следующем. По результатам исследования мы предлагаем рассматривать формирование культуры информационной безопасности менеджера поколения Z как результат взаимодействия трех контуров:

- индивидуального (психологические состояния и привычки цифровой гигиены);
- организационного (политики, процессы, лидерство, артефакты);
- технологического (безопасные по умолчанию инструменты).

При этом интернет-зависимость и цифровая тревожность выступают «усилителями» информационной безопасности в первом контуре, а грамотное проектирование вторых и третьих контуров гасит эти усилители. Зрелость культуры информационной безопасности измеряется устойчивостью безопасного поведения при дефиците времени и повышенной тревоге.

ЗАКЛЮЧЕНИЕ / CONCLUSION

В процессе проведенного исследования мы приходим к выводу о том, что культура информационной безопасности – не приложение к регламентам, но ядро управленческой практики цифровой организации. Для менеджеров поколения Z она выступает интерфейсом между их «всегда онлайн» когнитивным стилем и требованиями защищенности. Интернет-зависимость и цифровая тревожность, характерные для эпохи постоянной подключенности, меняют микродинамику решений и повышают вероятность нарушений информационной безопасности.

Интернет-зависимость и цифровая тревож-

ность представляют собой значимые социально-психологические вызовы для менеджеров поколения Z, которые находятся на пересечении высоких профессиональных требований и глубокой интеграции цифровых технологий в свою жизнь. Взаимоусиливающая связь между этими феноменами создает риски не только для индивидуального благополучия, но и для эффективности организационных процессов. Научные исследования в области психологии зависимостей, когнитивной психологии и организационного поведения предоставляют богатую основу для понимания механизмов развития и преодоления этих состояний.

Ключевыми выводами являются:

- интернет-зависимость и цифровая тревожность связаны с нейрокогнитивными изменениями, включая модификацию системы вознаграждения и исполнительных функций мозга;
- для менеджеров поколения Z характерны специфические формы проявления этих состояний, включая тревогу по поводу профессиональной онлайн-репутации, компульсивную проверку рабочих сообщений и страх упустить важную информацию;
- эффективные стратегии преодоления предполагают сочетание индивидуальных психологических техник (когнитивно-поведенческие стратегии, практики осознанности) и организационных мер, направленных на создание здоровой цифровой культуры;
- первостепенное значение имеет развитие информационной безопасности и «цифровой мудрости» – способности осознанно и избирательно использовать технологии для достижения значимых целей при сохранении психологического благополучия.

Перспективные направления дальнейших исследований включают:

- разработку и валидацию специфических диагностических инструментов для оценки цифровой тревожности в управленческом контексте;
- изучение долгосрочных последствий интернет-зависимости для карьерного развития менеджеров поколения Z;
- оценку эффективности различных организационных интервенций, направленных на поддержание цифрового благополучия и информационной безопасности.

Стоит отметить, что, несмотря на описанные риски, цифровые технологии сами по себе не являются источником социально-психологических проблем. Ключевое значение имеют качество и характер взаимодействия с ними. Развитие сбалансированного, осознанного подхода к ис-

пользованию технологий представляет собой важную задачу как для отдельных менеджеров, так и для социума в целом.

Высококвалифицированный, конкурентоспособный управленец – это не просто руководитель и образованная личность, но лидер, готовый к испытаниям, способный переучиваться и умеющий гибко реагировать и адаптироваться под

меняющиеся условия неопределенности и способный работать в них [Гасанова, Пожарская, Гасанов, 2024]. В этом контексте научное понимание социально-психологических факторов, влияющих на интернет-зависимость и цифровую тревожность, становится необходимой основой для создания и развития навыков цифровой грамотности и культуры информационной безопасности для защиты себя, своей организации и социума в целом от потенциальных рисков.

СПИСОК ЛИТЕРАТУРЫ

Бреслер М.Г., Алексеева Н.А. Живущие в цифровом мире. надежда и страх будущего у поколения Z. Социология. политология. международные отношения. 2024;2(8):165–173.

Гасанова З.Б., Гасанов М.И. Формирование цифровых компетенций у кадровых ресурсов как основа национальной безопасности. Экономика. Бизнес. Банки. 2024;1(71):69–79.

Гасанова З.Б., Пожарская Е.Л., Гасанов М.И. Подготовка управленческих кадров для цифровой экономики как фактор и гарант национальной безопасности государства. Экономика и предпринимательство. 2024;5(166):237–240.

Гасанова З.Б., Пожарская Е.Л. Социально-психологическая адаптация студентов в условиях цифровой экономики. Экономика и предпринимательство. 2022;7(144):1014–1018.

Краснянская Т.М., Тылец В.Г., Иохвидов В.В. Развитие проблематики информационно- психологической безопасности в современной отечественной психологии. Знание. Понимание. Умение. 2021;2:192–206. <https://doi.org/10.17805/zpu.2021.2.14>

Михеева М. Угрозы информационно-психологической безопасности личности менеджеров высшего звена. Вестник Московской международной академии. 2021.

Щербакова О.И., Осипов В.П. Современные вызовы социальной работы: проблема цифровой тревожности личности. В кн.: Проблемы социальной психологии и социальной работы: материалы XIX Всероссийской Парыгинской научно-практической конференции с международным участием. СПб; 2025. С. 33–35.

Barber L.K., Santuzzi A.M. Please respond ASAP: Workplace telepressure and employee recovery. Journal of Occupational Health Psychology. 2017;1(22):28–39.

Cheever N.A., Rosen L.D., Carrier L.M., Chavez A. (2018). Out of sight is not out of mind: The impact of restricting wireless mobile device use on anxiety levels among low, moderate and high users. Computers in Human Behavior. 2018;37:290–297.

Cheng C., Li A.Y. Internet addiction prevalence and quality of (real) life: A meta-analysis of 31 nations. Cyberpsychology, Behavior, and Social Networking. 2014;17(12):755–760.

Chun J., Shim H., Kim S. A meta-analysis of Internet addiction treatment methods among Korean adolescents. Cyberpsychology, Behavior, and Social Networking. 2017;4(20).

Elhai J.D., Dvorak R.D., Levine J.C., Hall B.J. Problematic smartphone use: A conceptual overview and systematic review of relations with anxiety and depression psychopathology. Journal of Affective Disorders. 2017.

Griffiths M.D. A ‘components’ model of addiction within a biopsychosocial framework. Journal of Substance Use. 2005;4(10):191–197.

Reidenberg J.R., Russell N.C., Halevy A. Privacy in the age of psychological targeting. Current Opinion in Psychology. 2015.

Sparrow B., Liu J., Wegner D.M. Google effects on memory: Cognitive consequences of having information at our fingertips. Science. 2011;333(6043):776–778.

Twenge J.M., Campbell W.K. Media use is linked to lower psychological well-being: Evidence from three datasets. Psychiatric Quarterly. 2019;2(90):311–331.

REFERENCES

Barber L.K., Santuzzi A.M. Please respond ASAP: Workplace telepressure and employee recovery. Journal of Occupational Health Psychology. 2017;1(22):28–39.

Bresler M.G., Alekseeva N.A. Living in the digital world. The hope and fear of the future for generation Z. Sociology. political science. international relations. 2024;2(8):165–173. (In Russian).

- Cheever N.A., Rosen L.D., Carrier L.M., Chavez A.* (2018). Out of sight is not out of mind: The impact of restricting wireless mobile device use on anxiety levels among low, moderate and high users. *Computers in Human Behavior*. 2018;37:290–297.
- Cheng C., Li A.Y.* Internet addiction prevalence and quality of (real) life: A meta-analysis of 31 nations. *Cyberpsychology, Behavior, and Social Networking*. 2014;17(12):755–760.
- Chun J., Shim H., Kim S.* A meta-analysis of Internet addiction treatment methods among Korean adolescents. *Cyberpsychology, Behavior, and Social Networking*. 2017;4(20).
- Elhai J.D., Dvorak R.D., Levine J.C., Hall B.J.* Problematic smartphone use: A conceptual overview and systematic review of relations with anxiety and depression psychopathology. *Journal of Affective Disorders*. 2017.
- Gasanova Z.B., Gasanov M.I.* Formation of digital competencies among human resources as the basis of national security. *Economy. Business. Banks*. 2024;1(71):69–79. (In Russian).
- Gasanova Z.B., Pozharskaya E.L.* Socio-psychological adaptation of students in the digital economy. *Journal of economics and entrepreneurship*. 2022;7(144):1014–1018. (In Russian).
- Gasanova Z.B., Pozharskaya E.L., Gasanov M.I.* Training of managerial personnel for the digital economy as a factor and guarantor of national security of the state. *Journal of economics and entrepreneurship*. 2024;5(166):237–240. (In Russian).
- Griffiths M.D.* A ‘components’ model of addiction within a biopsychosocial framework. *Journal of Substance Use*. 2005;4(10):191–197.
- Krasnianskaya T.M., Tylets V.G., Iokhvidov V.V.* The development of the problems of information and psychological security in modern Russian psychology. *Knowledge. Understanding. Ability*. 2021;2:192–206. (In Russian). <https://doi.org/10.17805/zpu.2021.2.14>
- Mikheeva M.* Threats to information and psychological security of senior managers’ personalities. *Bulletin of Moscow International Academy*. 2021. (In Russian).
- Reidenberg J.R., Russell N.C., Halevy A.* Privacy in the age of psychological targeting. *Current Opinion in Psychology*. 2015.
- Shcherbakova O.I., Osipov V.P.* Personality anxiety in the era of digitalization: from technophobia to digital anxiety. In: *Issue of social psychology and social activity: Proceedings of XIX All-Russian Parygin Scientific and Practical Conference with international participation*. 2025. Pp. 33–35. (In Russian).
- Sparrow B., Liu J., Wegner D.M.* Google effects on memory: Cognitive consequences of having information at our fingertips. *Science*. 2011;333(6043):776–778.
- Twenge J.M., Campbell W.K.* Media use is linked to lower psychological well-being: Evidence from three datasets. *Psychiatric Quarterly*. 2019;2(90):311–331.