INFORMATION SECURITY INSTITUTE

A NEW SECURITY PARADIGM

FOR FINANCIAL INSTITUTIONS

RESOLUTION

СПИКЕРЫ КРУГЛОГО СТОЛА:

LIST OF PARTICIPANTS WE ARE HONORED TO INVITE AS SPEAKERS:

Professor Harvey Wolf Kushner

Chairman of the Criminal Justice Department and a Professor of Criminal Justice at LIU Post, Brookville, New York. Internationally recognized expert on terrorism. Kushner has authored numerous columns, editorials, and six books, five of which focus on the pervasive problems inherent in international and transnational terrorism. His best-seller Encyclopedia of Terrorism has won numerous awards.

Dr. Oleg Maltsev

Author, criminologist, security expert, psychologist, photographer, and investigative journalist. He is a member of the presidium and academic researcher at the European Academy of Sciences in Ukraine (EUASU) and a member of the Ukrainian Academy of Sciences. He is an author of numerous books in areas such as applied history, sociology, depth psychology, philosophy, criminalistics, and criminology. He is an editor of several interdisciplinary peer-reviewed journals.

Professor Kathleen M. Carley

Professor in the School of Computer Science in the Carnegie Mellon Institute for Software Research at Carnegie Mellon University and also holds appointments in the Tepper School of Business, the Heinz College, the Department of Engineering and Public Policy, and the Department of Social and Decision Sciences. Director, CASOS Center at Carnegie Mellon University. Co-Director, Social Cyber-Security Working Group

Massimo Ortolani

Economist and economic consultant. He has been working in the ENI group, Mediocredito centrale and Unicredit group, with assignments mostly focused on international activities, assessment of geopolitical country risk and evaluation of investment projects. He has also worked as consultant in Latin America for UNIDO, and in Kazakhstan within EU programs. During the last decade has been focusing its research studies on geoeconomic risks, also as a lecturer on Economic Intelligence at the Tor Vergata University and Link Campus University of Rome. He is the author of "Economic Intelligence and Geoeconomic Conflict", among many other works.

Oliver Pahnecke

PhD candidate at Middlesex University. He obtained his LLM in International Business Law at Central European University, Budapest, and works as a fair trial expert for international organisations. He works as a rule of law expert for international missions and as a consultant for technical co-operation and finance.

Andrew Hoskins

EUASU Academician, Interdisciplinary Professor of Global Security in the College of Social Sciences, University of Glasgow UK. His latest book (with Matthew Ford) is Radical War: Data, Attention & Control in the Twenty-First Century (Hurst/OUP). He is founding Co-Editor-in-Chief of the Cambridge Journal of Memory, Mind & Media (2021-), founding Editor-in-Chief of the Sage Journal of Memory Studies (2008-), and founding Co-Editor-in-Chief of the Journal of Digital War (2020-).

Prof. Vitalii Lunov

Associate Professor in Bogomolets National Medical University. Presidium member and academician of European Academy of Sciences of Ukraine, Member of the American Psychological Association, the American Academy of Clinical Psychology, World Federation for Mental Health (USA), and the European Academy of Natural Sciences (Hannover, Germany).

Costantino Slobodyanuk

Presidium Member of EUASU. Associate fellow of the Ukrainian Academy of Sciences. Head of the Strategic council of the Information Security Institute. Head of Civil Society Organization Kavalyer. Editor-in-chief of the Newspaper Unsolved Crimes. He is engaged in the studies of online reputation management and security of enterprises.

Olga Panchenko

Corresponding Member of EUASU, attorney, and Director of Redut Law Company. n An associate fellow of the Ukraine Academy of Sciences. Chief editor of the Newsletter on the Results of Scholarly Work: in sociology, criminology, philosophy and political science. Journalist of the newspaper Unsolved Crimes. Presidium member of Odessa Scientific-Humanitarian Society and Historic-Literature Scientific Society.

Pavlo Pedina

EUASU expert, expert in finance, banking, insurance, and asset valuation. Financial consultant. Investment adviser for Slav Invest, financial director of MANORM Holding, and the head of the Paradox Credit Protection Society.

РЕЗОЛЮЦИЯ КРУГЛОГО СТОЛА

«Новая парадигма безопасности для финансовых учреждений»

(27.03.2023)

Данный документ представляет собой краткое изложение, выводы и основные аспекты международного научно-практического круглого стола, который состоялся в формате online 27 марта 2023 года на платформе **Information Security Institute** (ISI). В рамках данного мероприятия были рассмотрены некоторые из наиболее актуальных вопросов, которые касаются безопасности и ключевых уязвимостей в финансовом секторе, а именно:

1. Как стоит относиться к кибербезопасности, учитывая тот факт, что несмотря на многомиллионные вливания, этот инструментарий так и не решил ключевых проблем в отрасли?

2. Каким образом социальная кибербезопасность (как новое междисциплинарное научное направление) может помочь разрешить корневую проблему в финансовом секторе?

3. Как может выглядеть новая парадигма безопасности в финансовом секторе? Какие требования необходимо предъявить к новой парадигме, чтобы на этапе проектирования не допустить ошибку?

4. Как могла бы выглядеть соответствующая программа для повышения квалификации CISO (chief information security officer) для финансовых структур?

5. Какие отрасли, кроме финансовой, сегодня остро нуждаются в аналогичном подходе для разрешения своих технологических проблем?

Сегодня мы находимся в уникальной исторической точке, когда представители крупнейших консалтинговых компаний (McKinsey&Co), «большая четверка» аудиторских компаний (Deloitte, PWC, KPMG, EY) и целый ряд профильных структур (Merrill Lynch, Information Security Media Group, Proofpoint, Cyber Security Hub) вынужденно признают следующий факт: необходимо не только построить новую парадигму безопасности, но и найти решение по минимизации влияния человеческого фактора на успех бизнес-структур. Подробные статистические данные указанных выше структур мы рассмотрим во втором разделе резолюции.

Важно отметить ключевую тенденцию — несмотря на активный рост отрасли кибербезопасности, технологических проблем и уязвимостей в системе безопасности финансовых институтов не становится меньше. Кроме того, по мнению экспертов Института Информационной безопасности в финансовом секторе порядка 80% преступлений остаются «за кадром». В разных странах они могут по-разному квалифицироваться с точки зрения

локального уголовного законодательства. Однако у всех этих преступлений есть 2 общих признака: причиной этих преступлений являются либо инсайдерские угрозы, либо ошибки, допущенные сотрудниками финансовых структур. К сожалению, эти преступления никогда не станут достоянием общественности и потому, для экспертной среды они всегда будут находиться в «слепой зоне». С другой стороны, понятны причины и мотивы действий финансовых институтов. Любая огласка подобных случаев грозит серьезными репутационными рисками. В большинстве случаев подобные кейсы разрешаются в досудебном порядке урегулирования споров, в частности, благодаря механизму медиации. Таким образом, мы можем наблюдать лишь вершину айсберга тех реальных технологических проблем, с которыми сталкивается ежедневно финансовый сектор.

Международный научно-практический круглый стол «Новая парадигма безопасности для финансовых учреждений» создал все необходимые условия для конструктивного экспертного диалога на предмет разрешения текущих вызовов в отрасли безопасности. Кроме того, момент проведения круглого стола совпал с двумя неординарными событиями в финансовом секторе. Неожиданный финансовый коллапс американского «Silicon Valley Bank» и швейцарского «Credit Suisse» стал дополнительным маркером состояния турбулентности, в котором сейчас находится международный финансовый рынок. В очередной раз всем стало очевидно, что сегодня нет неприкасаемых, а человеческий фактор как и прежде, может иметь фатальное влияние на судьбу различных бизнес-структур. Серия ошибок, допущенных сотрудниками на уровне стратегического и тактического управления, может отправить на дно не только средних и небольших игроков, но и таких тяжеловесов в банковской сфере как «Silicon Valley Bank» и «Credit Suisse».

Ключевые выводы по итогам круглого стола

Вывод #1: Программы по минимизации влияния человеческого фактора должны занять одно из центральных мест в новой парадигме безопасности.

На протяжении многих лет западные специалисты в области безопасности принимали в качестве аксиомы «главенство технологий над человеческим фактором». Фактическая практика в сфере безопасности указывает на то, что без разрешения проблематики человеческого фактора, технологические решения не в состоянии обеспечить безопасность финансовых структур. В ходе круглого стола эксперты не только единогласно пришли к критической важности разработки программы по минимизации человеческого фактора, но и обсудили принципиальную модель построения такой программы. В частности, во время доклада **Dr. Олег Мальцев** представил модель, состоящую из трех элементов, которые должны существовать единовременно внутри любой организации или бизнес-структуры для построения максимально эффективной системы безопасности: *«Необходимо обеспе-*

чить научное наблюдение за потенциальной преступной средой (постоянное изучение и анализ); необходимо создать отдельный тренировочный центр, где подготовленные менеджеры, без использования каких-либо общедоступных программ, будут учить своих сотрудников; необходимо обеспечить регулярное повышение уровня подготовки отдельных сотрудников компании (special unit), так как потенциальный криминальный элемент, а также сам криминал свой уровень подготовки повышают постоянно. В основе построения системы безопасности лежит компетентность людей — только так можно эффективно защищаться как от внешних, так и от внутренних угроз».

Вывод #2: Новая парадигма безопасности должна быть сбалансированной

Кибербезопасность и система по минимизации человеческого фактора являются двумя центральными элементами в новой парадигме. Они являются взаимодополняющими, а не взаимоисключающими элементами. Любая попытка нарушить этот баланс будет приводить к иллюзии безопасности, это всегда приводит к крайне негативным последствиям и новым финансовым коллапсам.

В частности, в своем докладе итальянский **профессор Massimo Ortolani** отметил: *«В недавнем исследовании, проведенном Итальянской ассоциацией компаний по кибербезопасности "CLUSIT REPORT 2023", были представлены следующие выводы: очень важно найти баланс между первостепенной важностью человеческого фактора и усилиями по борьбе с киберпреступностью, которые по-прежнему должны будут опираться на использование технологических инструментов и приложений для обеспечения соответствия».*

Вывод #3: Необходимо в кратчайшие сроки разработать прикладную программу по минимизации влияния человеческого фактора.

Подобная программа, безусловно, должна быть мультидисциплинарной. Как отметил в своем докладе **Dr. Олег Мальцев**: *«Современная парадигма безопасности не связана со специализацией, потому что в нашем трансформирующемся мире может произойти все что угодно. Специалиста в области безопасности изготавливают как дорогой ключ к дорогому и сложному замку. Карьера такого специалиста движется от приобретения навыков и повышения уровня подготовки к уровню преподавателя / эксперта и далее движется к ученому. Никакая другая система безопасности сегодня не является эффективной».*

Профессор Andrew Hoskins подчеркнул дополнительную угрозу в лице databrokers, которую необходимо учесть при разработке программы. Речь идет не только про обеспечение безопасного хранения и конфиденциальности информации, но и про различные методы воздействия на сотрудников бизнес-структур со стороны databrokers из darkindustry.

Кроме того эксперты сошлись во мнении, что подобная программа является жизненно необходимой не только для банковского сектора, но и для целого ряда других отраслей рынка. В частности **Oliver Pahnecke** отметил, что среди наиболее чувствительных к человеческому фактору категорий бизнеса стоит выделить следующие: медицинская отрасль, сфера образования, Big Data Companies, энергетическая отрасль, страховые компании, кредитные союзы, стартапы. По мере разработки программы, список отраслей, вероятно, будет расширяться.

Вывод #4: На этапе разработки программы, следует учесть три ключевых требования.

По итогам проведения круглого стола эксперты сформулировали следующие требования к будущей программе:

1. Отказ от масс-маркет инструментов;
2. Строгое соблюдение баланса интересов наемных сотрудников и работодателей;
3. Многофункциональность — программа должна не только указывать на уязвимости и скрытые угрозы, но и выявлять точки роста компании в аспекте надежных и перспективных сотрудников.

Первое требование напрямую связано с тем, что любые масс-маркет инструменты с точки зрения безопасности имеют потенциал критической угрозы. Подобные общедоступные инструменты, в частности, создают благоприятные условия для инфильтрации в бизнес недобросовестных сотрудников и представителей криминальных субкультур. Как отметил **профессор Harvey Wolf Kushner**: «*За последнее время сфера безопасности очень изменилась. Я знаю, что многие коллапсы в компаниях возникают из-за человеческого фактора и отсутствия необходимой подготовки сотрудников. Поэтому в рамках новой программы необходимы специальные инструменты, которые доступны не всем, это не масс-маркет. И я бы хотел участвовать в создании системы, где главную роль играет отбор кадров. Такая система необходима сейчас для финансового сектора, для банков, для страховой отрасли и т.д. И самое главное – упор в системе нужно делать на устранение человеческого фактора*».

Второе требование сформулировала **адвокат Ольга Панченко**: «*Для того чтобы минимизировать человеческий фактор, необходимы руководящие инструкции, а не рекомендательные. И здесь может возникнуть вопрос, будет ли это нарушать права человека, не будет ли это дискриминацией. Когда речь идет об индивидуальной ответственности, то деятельность человека не ведет к последствиям для коллектива. Но когда речь идет о групповой тенденции – все меняется, то есть рекомендательных инструкций уже недостаточно, необходимы руководящие инструкции.*

Парадигма, которую мы предлагаем, безусловно, содержит в себе именно руководящие инструкции с одной стороны, с другой – она, безусловно, будет содержать баланс прав наемных сотрудников и работодателей, что исключает какую-либо дискриминацию».

Третье требование связано с тем, чтобы на этапе внедрения программы в бизнес-структуры, необходимо максимально исключить фактор предубежденности со стороны сотрудников. Как отметил **Oliver Pahnecke** подобная программа должна стать не только важным инструментом для владельцев и топ-менеджеров бизнес-структур по выявлению существующих / скрытых / потенциальных угроз, связанных с человеческим фактором. Она также должна стать твердой опорой для эффективных сотрудников компании, которые благодаря этой программе смогут ускорить свое вертикальное движение по карьерной лестнице. По своей природе программа должна быть абсолютно нейтральна. Главной задачей является минимизация влияния человеческого фактора на краткосрочный и долгосрочный успех бизнес-структур.

Вывод #5: Человеческий фактор следует рассматривать исключительно как систему.

Employee Selection, Insider threats, Behavioral stress и Human errors — именно эти четыре элемента совокупно создают систему человеческого фактора, которую в рамках круглого стола предложил к рассмотрению **криминолог Константин Слободянюк.**

Эксперты не только поддержали такой 4-element approach к работе с человеческим фактором, но и пришли к единому мнению о том, что любая попытка упростить эту целостную систему до уровня рассмотрения отдельных элементов, будет приводить к иллюзии безопасности и финансовым коллапсам.

Со своей стороны **профессор Виталий Лунев** отметил, что с точки зрения психодиагностики в рамках новой программы придется комбинировать психометрические инструменты, проективные методики и навокальные тесты: «*Когда речь идёт про Employee Selection и Behavioral stress будет работать следующая зависимость — чем более высокую должность занимает сотрудник в иерархии компании, тем больше придется использовать проективных методик для получения объективной информации для принятия решений и внесения необходимых изменений.*

Уровень сотрудника в иерархии определяет объем ответственности, уровни допуска к конфиденциальной информации и объём давления, который на него оказывается. Именно поэтому для построения объективных прогнозных моделей поведения сотрудников, нам придется использовать как проективные психодиагностические методики, так и навокальные тесты».

Статистика и публичный консенсус

Публичный консенсус по вопросу человеческого фактора стал результатом серии отчётов, которые были инициированы не только государственными структурами, но и ведущими организациями по кибербезопасности, финансовыми учреждениями, CISO, а также аналитическими и экспертными компаниями. Главный вывод сводится к необходимости разрешения ключевой проблемы в сфере безопасности, а именно – человеческого фактора.

Как уже было отмечено ранее, сегодня мы находимся в уникальной исторической точке, когда представители крупнейших консалтинговых компаний (McKinsey&Co), «большая четверка» аудиторских компаний (Deloitte, PWC, KPMG, EY), и целый ряд профильных структур (Merrill Lynch, Information Security Media Group, Proofpoint, Cyber Security Hub) вынужденно признают тот факт, что следует найти системное решение по минимизации влияния человеческого фактора. В ходе подготовки к круглому столу было изучено более 50 отчетов различных структур. Обзор статистики и аналитики был представлен финансовым экспертом Павлом Пединой:

- Причина 95% нарушений безопасности во всем мире в человеческом факторе *(отчет **WEF** «The Global Risks Report 2022»);*

- 82% зарегистрированных кибератак связаны с человеческим фактором (отчет Proofpoint «Cybersecurity: The 2022 Board Perspective»);

- На 44% выросло число инцидентов, связанных с инсайдерскими угрозами *(отчет **Ponemon Intsitute** «2022 COST of Insider Threats»);*

- 4,24 миллиона долларов - средняя стоимость утечки данных *(отчет **Ponemon Institute** «2022 COST of Insider Threats»);*

- Согласно исследований **IBM**, 95% нарушений в системе кибербезопасности, которые приводят к кибервзломам, происходят по вине человека;

- *«Человеческий фактор является основной причиной финансовых преступлений»*. Так звучит основной вывод Управления финансового надзора (FCA), который был опубликован в «Руководстве по борьбе с финансовыми преступлениями»;

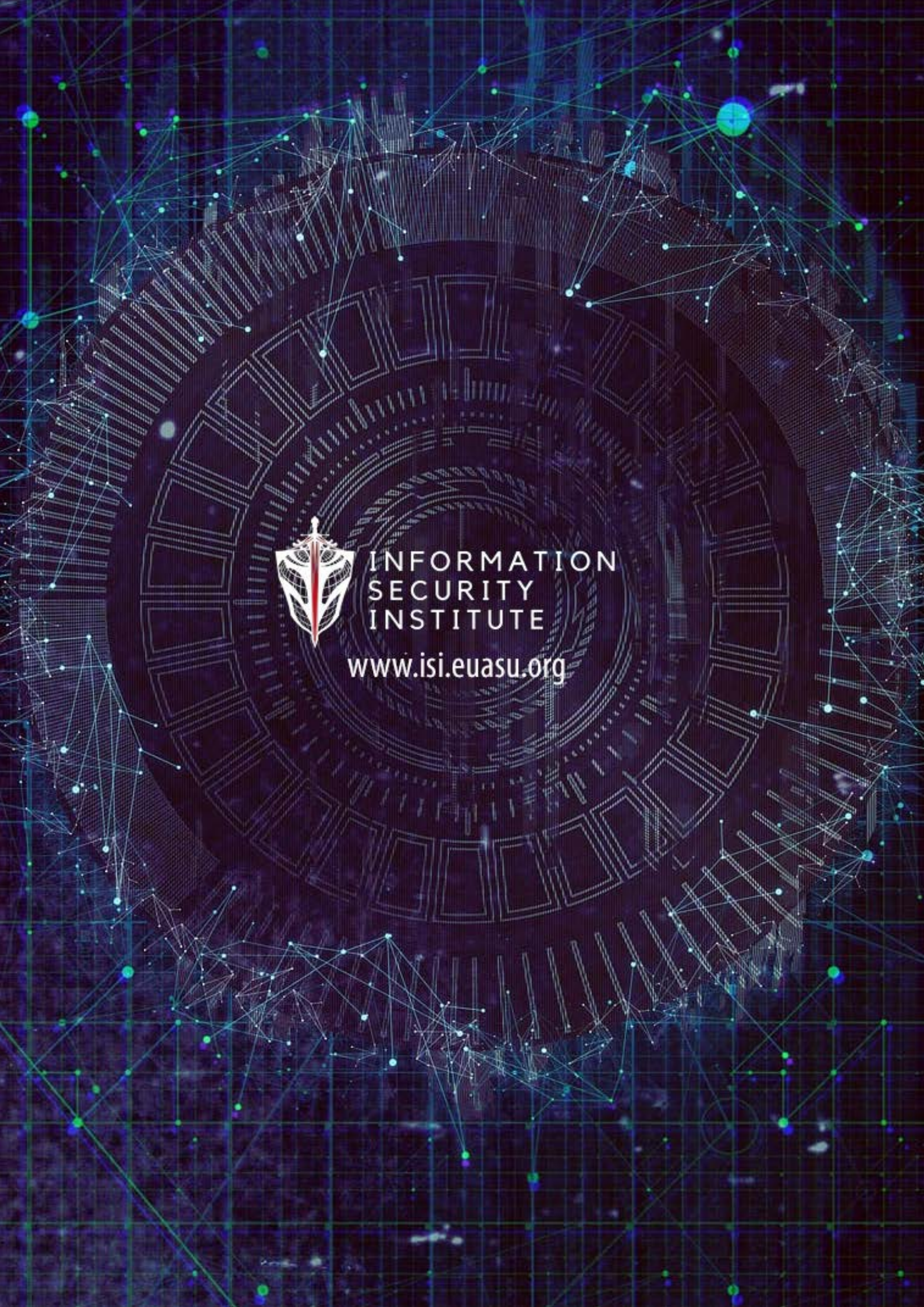
- **McKinsey&Co:** «Киберпреступники все чаще нацеливаются на сотрудников и других инсайдеров, используя методы социальной инженерии, чтобы обманом заставить их разгласить конфиденциальную информацию или предоставить доступ к системам. Поведение сотрудников и внутренние угрозы являются одними из наиболее значительных рисков для кибербезопасности организации». Источник: «Защита критически важных цифровых активов: не все системы и данные одинаковы» (McKinsey&Co);

- **KPMG**: «Финансовые преступления часто совершаются при активном участии или пособничестве банковских служащих либо с использованием недостатков системы внутреннего контроля. 88% случаев финансовых преступлений, о которых сообщалось KPMG, были связаны с участием или сговором сотрудников».Источник: «Ясность финансовых преступлений в банковской сфере» (KPMG);

- **PwC:** в статье «Глобальный обзор экономических преступлений PwC 2021: превращение риска в устойчивость» отмечается, что почти половина всех экономических преступлений совершается внутренними субъектами;

- **Deloitte**: в статье «Управление рисками финансовых преступлений» отмечается что инсайдерские угрозы представляют значительный риск для организаций.

Таким образом, резюмируя вышесказанное, с гордостью заявляем, что на базе «Института Информационной безопасности» (ISI) в течение ближайших нескольких месяцев будет разработана программа по минимизации влияния человеческого фактора. В экспертную группу войдут специалисты из разных экспертных и научных областей, таких как: безопасность, психология, криминология, уголовная юстиция, информационная безопасность, менталитетная составляющая, экономика и финансы, а также права человека. Возглавит экспертную группу — научный руководитель ISI **Dr. Олег Мальцев.**


INFORMATION
SECURITY
INSTITUTE
www.isi.euasu.org