DOI: 10.25728/mlsd.2023.1161

СЦЕНАРНЫЙ ПОДХОД К ПРОТИВОДЕЙСТВИЮ ПОЧТОВЫМ ФИШИНГОВЫМ АТАКАМ В СФЕРЕ БИЗНЕСА

Фейзов В.Р.
Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
vadimus150@gmail.com

Аннотация. Данная работа представляет собой междисциплинарное исследование в области кибербезопасности, в котором анализируется влияние поведенческих факторов сотрудников на уровень уязвимости перед почтовыми фишинговыми атаками, применяя различные сценарии. В ходе исследования учитываются психологические особенности сотрудников из разных отделов компании и оценивается их влияние на предрасположенность к фишинговым атакам. Автор предлагает подход, позволяющий компаниям разработать более эффективные стратегии противодействия фишингу. Данный подход помогает определить уникальные психологические и поведенческие паттерны, которые могут служить как факторы риска в контексте фишинговых атак.

Ключевые слова: сценарный анализ, когнитивные карты, информационная безопасность, фишинговые атаки, управление персоналом, психологические черты личности.

Введение

Генеральный секретарь ООН, Антониу Гутерриш, подчеркнул, что социальные сети и другие цифровые платформы трансформируются из средств глобального общения в источники страха и дезинформации. Этому утверждению сложно противоречить, учитывая, что социальные сети, в первую очередь, служат источниками информации для планирования и организации подобного рода атак. От мошенников до разведывательных структур, многие активно используют открытые источники для сбора информации о гражданах или населении в целом. С развитием социальных сетей эволюционируют и методы сбора и обработки информации. Несомненно, информационная грамотность населения повышается со временем, однако в контексте постоянного привлечения новых слоев населения, темпы повышения осведомленности граждан остаются недостаточными, несмотря на своевременные изменения в законодательстве данной сферы.

За последние годы наблюдается рост количества утечек персональных данных граждан, что во многом связано с условиями обеспечения информационной безопасности и развитием тактик и инструментов злоумышленников. В Российской Федерации сложность ситуации усугублялась излишней толерантностью наказаний за подобные нарушения. До 2023 года компании, допустившие утечку информации согласно пункту КоАП 13.11, подвергались штрафам максимум на 600 тыс. рублей при повторном нарушении и до 100 тыс. рублей при первичном. Поэтому европейский опыт регулирования сферы персональных данных кажется более привлекательным, поскольку GDPR (Генеральный регламент о защите данных Европейского Союза) предусматривает штрафы до 4% от оборота компании-нарушителя за несоблюдение мер защиты информации, что привело к утечке персональных данных. Однако контроль за утечками в европейском пространстве не ограничивается этим: компания-нарушитель обязана в течение 72 часов сообщить о произошедшей утечке не только регулирующему органу, но и потребителям. В то же время, регулирующие органы замечают подобные недостатки и стремятся их устранить. На момент 2023 года Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации подготовило поправки в законы, предусматривающие оборотные штрафы до 3% для компаний-нарушителей.

Утечки персональных данных представляют собой значительную угрозу, однако для организации кампаний по дезинформации или специализированных атак требуется больше информации о сотруднике или организации. Данные, полученные любыми доступными методами, — это лишь начальный этап в стратегии злоумышленников. От телефонного мошенничества до рассылки фишинговых писем, любая целенаправленная атака становится более эффективной при наличии дополнительной информации о цели.

Согласно статистике Лаборатории Касперского, 48,63% писем глобально и 52,78% писем в сегменте Российского интернета являются спамом. Важно разграничивать обычный спам и фишинг: спам может включать в себя некоммерческую рекламу, в то время как фишинг имеет цель сбора данных с последующей их перепродажей или использованием для мошеннических целей. Тем не менее, массовые рассылки фишинговых писем классифицируются как спам-рассылки. Фишинговые атаки представляют собой одну из форм социальной инженерии, и, поэтому, считается, что повышение

уровня осведомленности сотрудников может уменьшить количество успешных атак. Обеспечение информационной безопасности предприятия требует тщательного мониторинга сотрудников и их уровня подготовки. Это включает не только классическое обучение основам информационной безопасности, но и мониторинг состояния сотрудников. В корпоративном контексте существуют различные виды фишинговых атак, включая целевой фишинг, почтовый фишинг, веб-фишинг, атаки методом «злой двойник», и вишинг (телефонный фишинг). Это не полный перечень всех возможных атак, но он демонстрирует наиболее вероятные векторы атак, связанные с социальной инженерией.

Основным направлением данной работы является решение проблемы противодействия почтовому фишингу посредством совершенствования управления корпоративной безопасностью. Задачей исследования является исследование возможностей сценарного анализа в управлении информационной безопасностью предприятия. Сценарный анализ, в основе которого лежит математический аппарат знаковых, взвешенных и функциональных графов является инструментом оценки поведения сложной системы при различных управленческих воздействиях и влияниях внешней среды. Сценарный подход позволяет на качественном уровне исследовать широкий спектр событий и факторов, влияющих как прямо, так и косвенно на реализацию целей управления. Анализ результатов, полученных в ходе сценарного моделирования в рамках проведенного исследования, позволил корректировать подходы к управлению безопасностью предприятия, включая изменение политики информационной безопасности и организацию целевых мероприятий по защите информации. Такой подход позволяет достигать наиболее эффективных решений, адаптированных к изменяющейся ситуации и исходным условиям.

1. Психологические черты и состояние сотрудников

Учитывая тот факт, что почтовый фишинг преимущественно нацелен на сотрудников организации, необходимо изучить факторы, влияющие на их поведение и реакции. Такие атаки обладают широким распространением в корпоративной среде, поскольку при успешной реализации они могут нанести значительный ущерб компании. Схематичное представление типичной атаки и возможной реакции на нее приведено на рис. 1.

Рис. 1. Классическая схема почтового фишинга

На представленной схеме обозначена концепция, согласно которой сочетание превентивной работы с персоналом и использование технических средств защиты обеспечивает противодействие кибератакам на этапе, где потенциальный ущерб для организации еще минимален, если не отсутствует вообще. Эта идея формирует стратегии обеспечения информационной безопасности в бизнесе. Хотя в статье основное внимание уделяется работе с персоналом, а технические средства защиты информации упоминаются более чем кратко, значение последних не следует приуменьшать. Даже наиболее обученный и осведомленный персонал не сможет обеспечить безопасность без поддержки высокотехнологичных решений, включая антивирусные программы, системы контроля утечек данных, различные фильтры, брандмауэры, шлюзы безопасности, системы многофакторной аутентификации, системы предотвращения и обнаружения вторжений, а также технологии искусственного интеллекта. Аналогично, необходимо подчеркнуть, что даже при использовании полного спектра средств защиты информации, персонал остается уязвимым звеном и способны привести к нарушениям

информационной безопасности. Это может проявляться в виде ошибок, неверных действий, недостатка знаний или понимания, а также в связи с утечками информации. Правильно настроенная техническая защита, сочетающаяся с обучением и контролем персонала, способно стать основой для минимизации расходов на устранение последствий утечек информации и восстановление работы после возможных кибератак.

Схема атаки в корпоративной сфере не существенно отличается от классического интернет-фишинга или обычного спама, поскольку все эти методики основываются на принципах социальной инженерии. В этой связи, целесообразно выделить ключевые персональные характеристики сотрудника или коллектива для формирования эффективного ответа на такого рода угрозы.

Исходя из типовых видов фишинговых атак, можно сделать вывод, что атаки целенаправленно используют определенные паттерны человеческого поведения или состояния, в частности, восемь из них: невнимательность, любопытство, страх, жадность, доверие, послушание, невежество и взаимность. Здесь стоит уточнить, что под «страхом» подразумевается эмпирический страх или страх последствий своих действий. Именно такие модели поведения и реакции на поступающие фишинговые письма представляют интерес для данного исследования. Для анализа предрасположенности сотрудников к такому поведению важно определить ключевые черты их личности, которые включают следующие аспекты: (1) Организованность; (2) Способность к творчеству; (3) Умение системно мыслить; (4) Отношение к риску; (5) Психологическая устойчивость; (6) Рационализм (прагматизм); (7) Адаптивность; (8) Конформизм; (9) Решительность; (10) Уровень оптимизма; (11) Коммуникативность; (12) Отношение к авторитету; (13) Образование и эрудиция; (14) Эмоциональность; (15) Самоуважение; (16) Клановость; (17) Независимость мышления; (18) Усердие; (19) Самопожертвование; (20) Упрямство; (21) Самодовольство; (22) Импульсивность; (23) Низкий самоконтроль; (24) Самоуверенность.

Несмотря на существование более обширного списка характеристик, выделенные 24 черты личности особенно значимы в контексте влияния на паттерны поведения, обозначенные выше [1-4]. Процесс сбора таких данных о сотрудниках является затратным и затруднительным. Его сложность определяется не только необходимостью привлечения внутренних и внешних специалистов и использования специализированных инструментов для анализа, но также усугубляется стремлением сотрудников минимизировать распространение персональной информации. С юридической точки зрения, законодательство защищает работников от неправомерного сбора подобной информации. Однако, существуют методики, которые могут быть применены руководителями компаний или сотрудниками отделов кадров в соответствии с их целями и задачами.

Одним из доступных подходов является поведенческий анализ, который включает самоотчетность сотрудника, оценку со стороны руководства и обратную связь от коллег. Несмотря на то, что восприятие коллег может быть некоторым образом субъективно и не всегда точно отражает психологические черты личности, такая методика как самоотчетность, подразумевающая использование специализированных инструментов оценки личности (например, DISC, тест Майерса-Бриггса, MMPI и т.д.) в форме тестов, обеспечивает более точную оценку. Проведение такого анализа может быть еще более эффективным при привлечении профессионального психолога для внешнего аудита. Технические методы, такие как сбор данных с рабочего компьютера, также могут быть эффективными. Это позволяет анализировать тексты электронных писем, сообщений и других форм текстовых коммуникаций. Вопрос нарушения конфиденциальности и этических норм в этом контексте не уместен, поскольку речь идет исключительно о деловой переписке внутри компании и с бизнес-партнерами. Использование искусственного интеллекта и машинного обучения позволяет анализировать большие объемы данных, включая публичные аккаунты в социальных сетях сотрудников. Сотрудники отдела кадров могут внимательно изучить ответы потенциальных сотрудников на собеседовании и организовывать специализированные тренинги и семинары по информационной безопасности для повышения их квалификации, а также сбора информации и определения некоторых аспектов их личности. Среди специфических методик можно выделить анализ ключевых показателей эффективности (KPI) и назначение специальных супервайзеров, включая область информационной безопасности. Однако ввиду затратности такого подхода, рекомендуется использовать его, как и внешний аудит, только при наличии проблем с внутренними проверками безопасности или при неэффективном сборе данных.

2. Сценарное моделирование

Основу данной работы составляет модель цифрового портрета гражданина в сети, представленная в 2022 году [5], которая описывает общие черты личности, воздействуя на которые возможно оказать необходимое влияние на индивидуума. Сценарная модель является начальным этапом сценарного анализа для исследования процессов, связанных с безопасностью личности и предприятия в целом. Настоящее исследование представляет собой продолжение представленной ранее работы и фокусируется на более специфических угрозах.

Целью данного моделирования является оценка вероятности успешной реализации фишинговой атаки, исходя из поведения восьми основных факторов. Представленная модель носит теоретический характер, при этом управленческие решения, а также исходные показатели представляют собой абстрактные данные. Для иллюстрации данного подхода и его функционала принято решение сформировать три различные группы работников в рамках одного предприятия. В качестве основы для формирования характеристик отдела маркетинга [6-7], кадрового отдела [8-12], а также отдела информационных технологий [13-15] были использованы результаты исследований, связанные с профессиональной сферой деятельности соответствующих групп, а также общие данные о требованиях, необходимых для адекватного выполнения задач. Характеристики сформированных групп приведены в таблице ниже. Значение «+» в каждой ячейке таблицы обозначает то, что представленная психологическая черта соответствует группе, «-» означает отсутствие соответствия.

Таблица 1. Соотношение групп работников и их психологических характеристик

Черта характера	**Отдел маркетинга**	**Кадровый отдел**	**Отдел информационных технологий**
Организованность	+	+	+
Способной к творчеству	+	-	+
Умение системно мыслить	-	-	+
Отношение к риску	+	-	-
Психологическая устойчивость	+	+	+
Рационализм (прагматизм)	-	+	-
Адаптивность	+	+	+
Конформизм	-	+	-
Решительность	+	-	+
Уровень оптимизма	+	+	-
Коммуникативность	+	+	-
Отношение к авторитету	-	+	-
Образование и эрудиция	+	-	+
Эмоциональность	+	-	-
Самоуважение	+	+	+

Черта характера	**Отдел маркетинга**	**Кадровый отдел**	**Отдел информационных технологий**
Клановость	-	+	+
Независимость мышления	+	-	+
Усердие	+	+	+
Самопожертвование	-	-	+
Упрямство	-	-	+
Самодовольство	-	-	+
Импульсивность	+	-	-
Низкий самоконтроль	-	+	-
Самоуверенность	+	+	+

Модель включает в себя 4 группы факторов, обозначенные на рис. 2-7 римскими цифрами (I-IV). Группы I и IV представляют собой «гибкие группы», что подразумевает возможность изменения их вершин. Например, первая группа служит исключительно для входных данных. Как видно из рис.2, при подаче единичного импульса через активацию мета-вершины «Отдел маркетинга», каждый импульс поступает в вершину второй группы, в соответствии с данными, указанными в таблице. Четвертая группа также является гибкой, поскольку включает факторы, связанные с управлением персоналом. В зависимости от поведения факторов третьей группы, что является основной целью моделирования, меняется группа IV, так как управление персоналом корректируется на основе результатов моделирования. Группы II и III являются статическими, и их вершины не меняются, так как они соответствуют представленным источникам. На рис. 2 можно также увидеть, что при отсутствии активации группы IV (мета-вершина «Сбор и мониторинг данных о состоянии сотрудников» выключена), фактор «Компрометация электронной почты» увеличивается. Это указывает на то, что данная группа работников находится в зоне риска, и возможность успешной реализации фишинговой атаки по определенным паттернам возрастает.

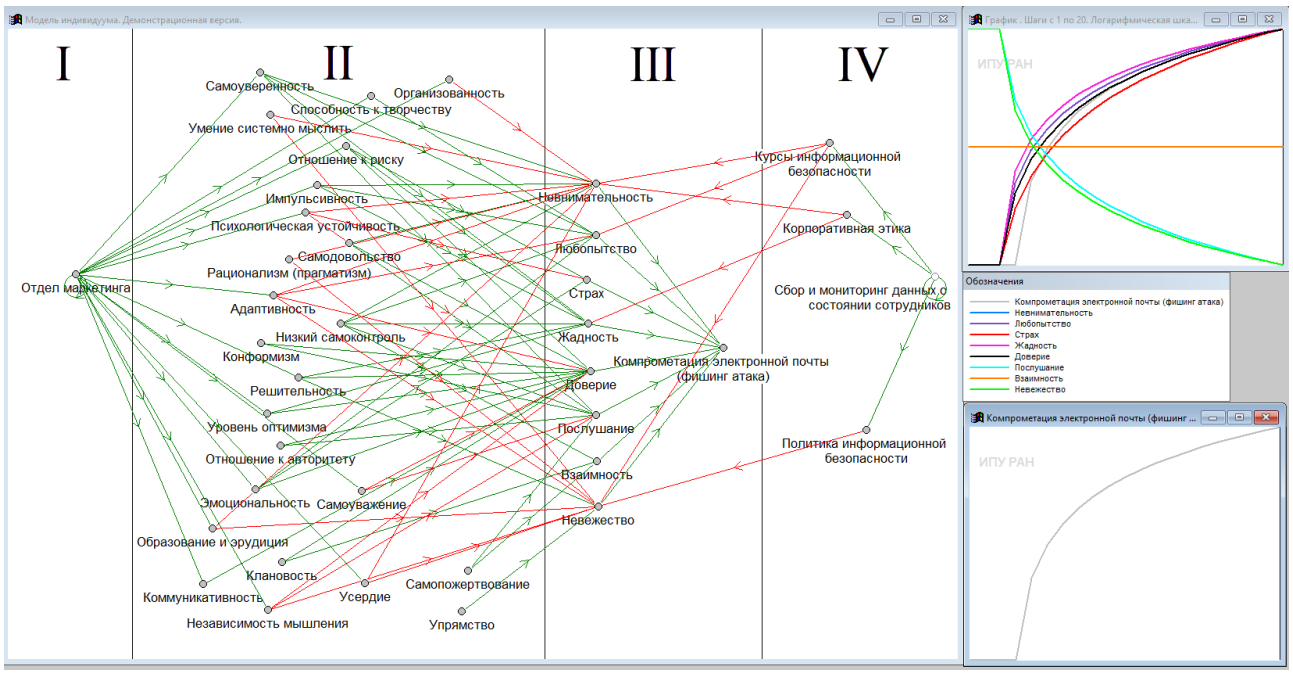

Рис. 2. Отдел маркетинга без управления безопасностью предприятия

Анализ полученных данных показывает, что в группе (III) факторы «Страх», «Доверие», «Любопытство» и «Жадность» оказывают значительное влияние на итоговый результат. В таких условиях для противодействия атакам используется четвертая группа факторов (IV), связанная с управлением сотрудниками. Управление, в контексте безопасности, строится на основе политики, этики и обучения сотрудников предприятия.

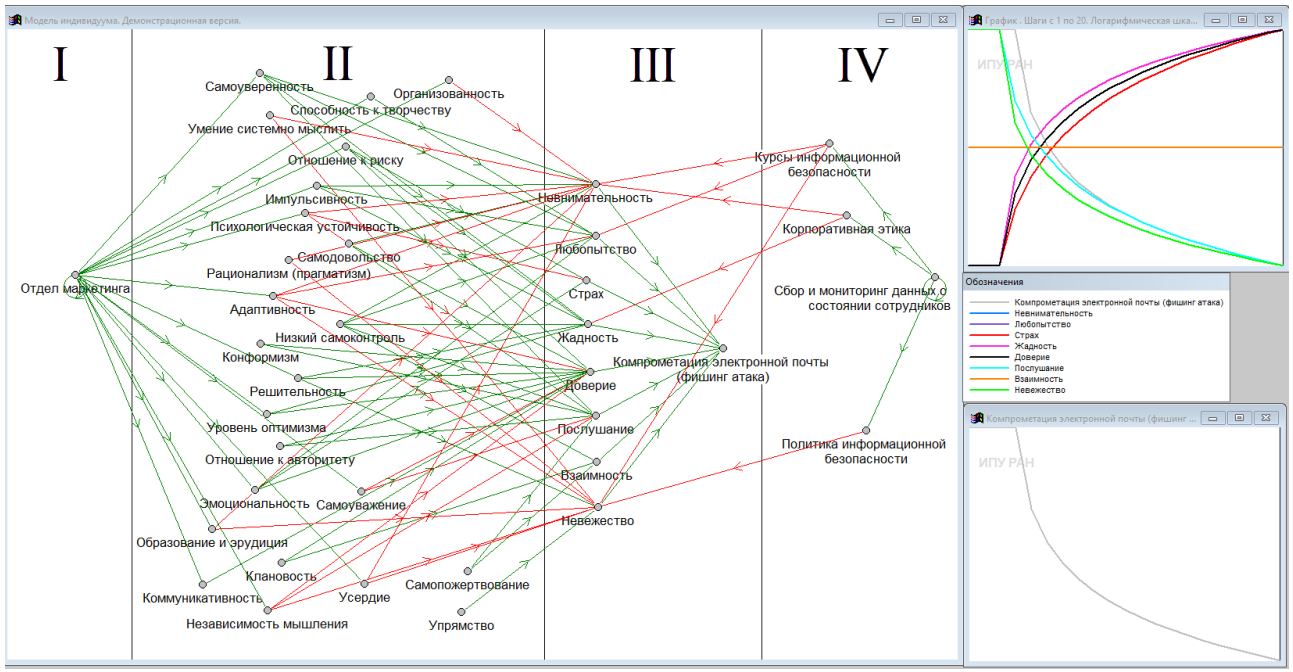

Рис. 3. Отдел маркетинга с управлением безопасностью предприятия

Активизация мета-вершины «Сбор и мониторинг данных о состоянии сотрудников» генерирует единичный импульс, который воздействует на вершины, связанные с управлением безопасностью предприятия. Это влияние отражается на ключевых вершинах третьей группы (III) и приводит к снижению показателя «Компрометация электронной почты». Стоит учесть, что четвертая группа (IV) сформирована исключительно для демонстрационных целей, так как выбор конкретных управленческих решений зависит от специфики каждого предприятия и возможности их реализации. В данном случае, выбранная стратегия обеспечения безопасности направлена на борьбу с

невнимательностью, излишним любопытством и невежеством сотрудников через специализированные курсы информационной безопасности. Противодействие же паттерну поведения «жадность» осуществляется посредством использования соответствующей корпоративной этики.

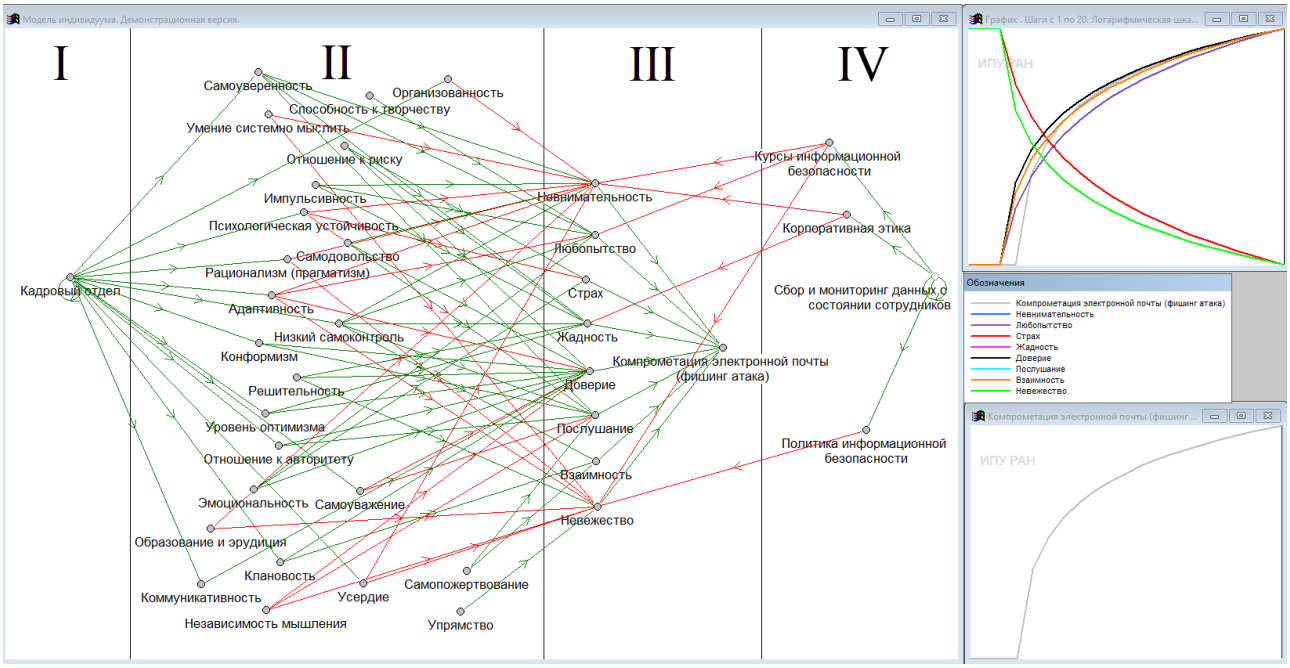

Рис. 4. Кадровый отдел без управления безопасностью предприятия

Рис. 4 представляет собой аналогичную модель с использованием входных данных другого отдела. Как показано, без какого-либо воздействия лишь факторы «Страх» и «Невежество» не являются уязвимыми в данной группе работников. Показатель компрометации в таком случае возрастает.

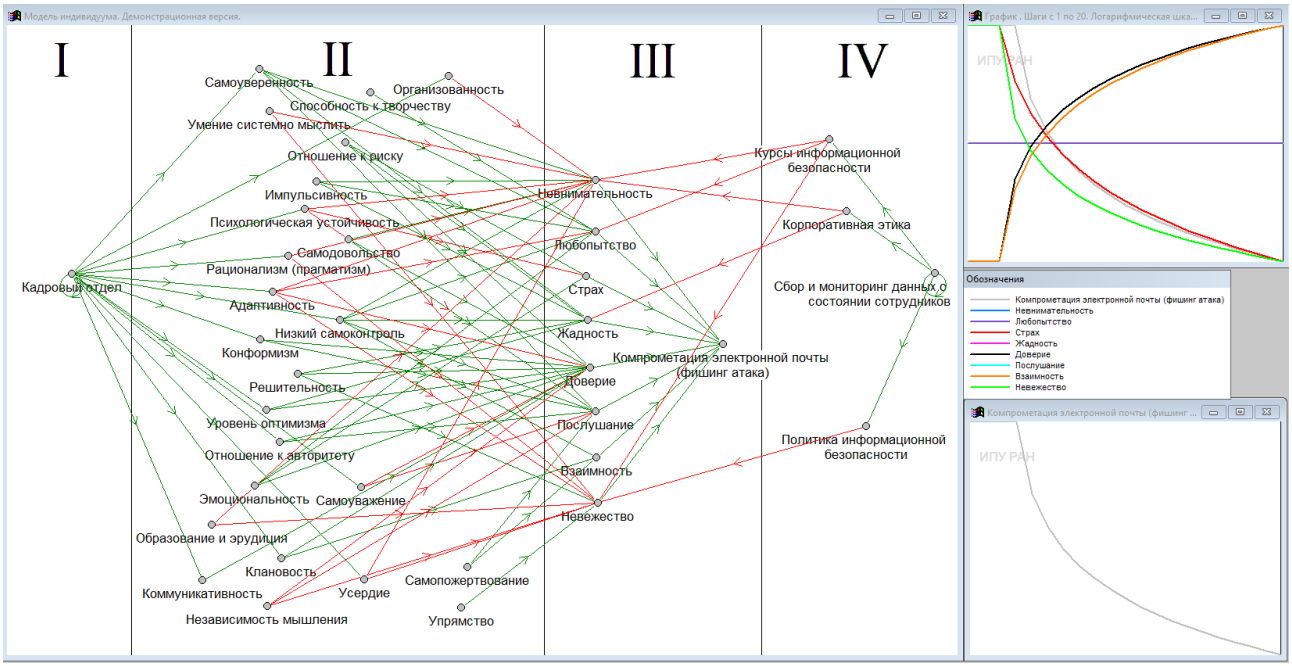

Рис. 5. Кадровый отдел с управлением безопасностью предприятия

Рис. 5 демонстрирует изменение прогноза возможности успешного осуществления фишинговой атаки в кадровом отделе. С активацией мета-вершины, связанной с обеспечением безопасности, ситуация становится более стабильной. Однако модель указывает на то, что такие факторы как «Доверие» и «Взаимность» все еще остаются на высоком уровне в анализируемой группе. Это свидетельствует о том, что, хотя общая вероятность успешного проведения атаки снижается, это

касается только некоторых из паттернов, представленных в модели. Поэтому, в этой ситуации требуется дальнейшая корректировка организационных или технических мер обеспечения безопасности на предприятии с учетом оставшихся векторов атаки.

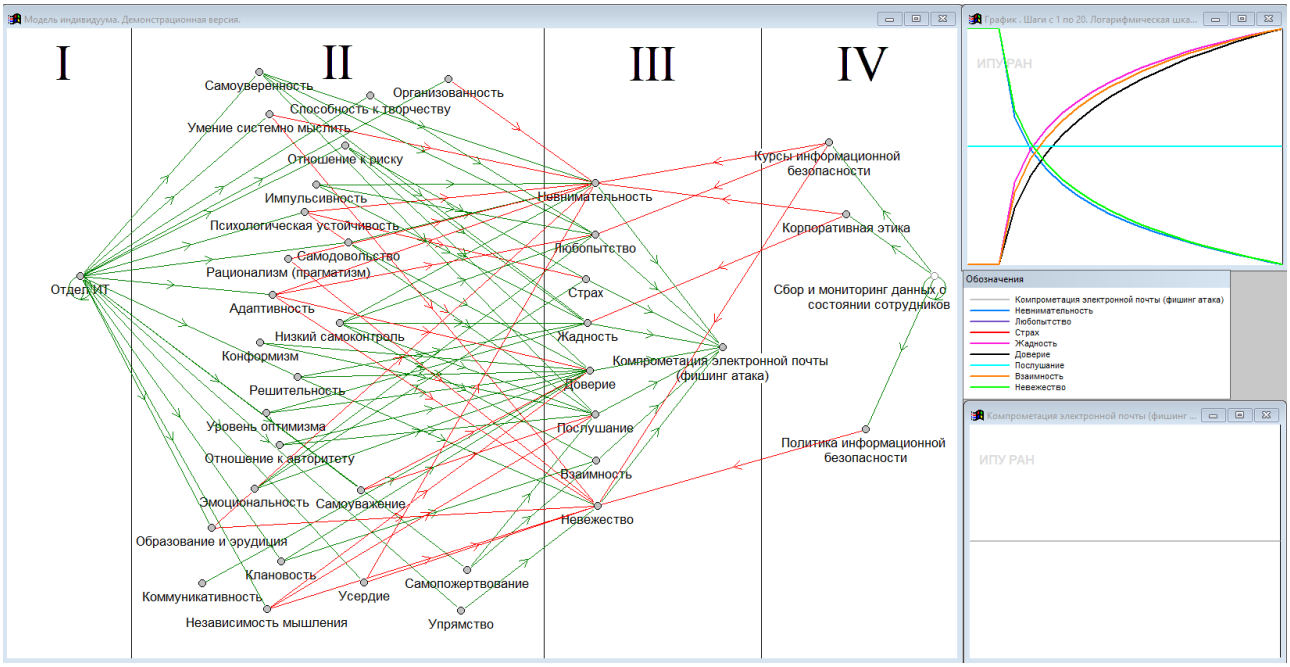

Рис. 6. Отдел информационных технологий без управления безопасностью предприятия

На Рис. 6 представлено новое состояние модели, при котором через группу факторов (I) анализируется отдел информационных технологий. Стоит отметить, что суммарная оценка успешного осуществления атаки находится на пограничном уровне (прямая линия на графике), обусловленным взаимной компенсацией положительных и отрицательных влияний на фактор компрометации электронной почты. Однако при отдельном рассмотрении поведения каждого фактора становится понятно, что даже если вероятность реализации такого рода атаки в сравнении с другими исследуемыми группами относительно низка, отсутствием угрозы это не гарантирует. В этом контексте требуется также корректно организовать мероприятия по обеспечению безопасности, учитывая, что факторы «Доверие», «Взаимность» и «Жадность» демонстрируют наибольший прирост и, таким образом, эти паттерны поведения представляют собой потенциальные уязвимости.

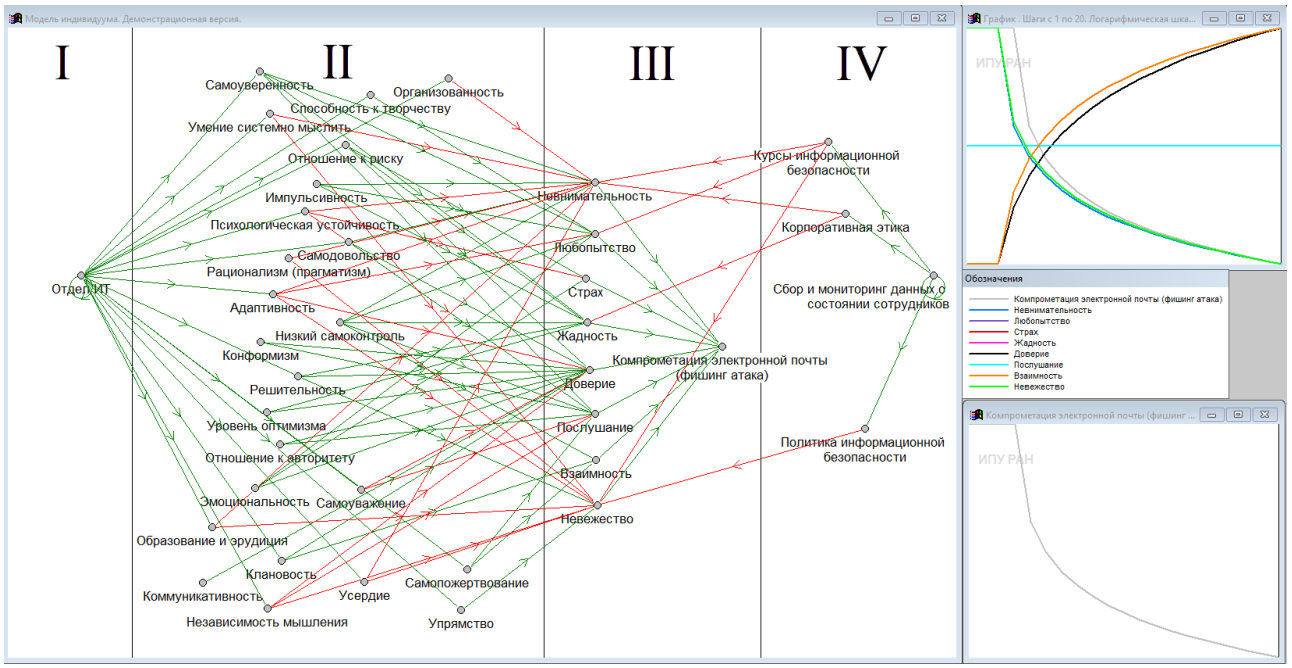

Рис. 7. Отдел информационных технологий с управлением безопасностью предприятия

Использование соответствующих методов обеспечения безопасности позволило улучшить общую ситуацию, однако, как видно из рис. 7, не все факторы были учтены данной стратегией.

Важно подчеркнуть, что модель не учитывает возрастные показатели работников, хотя они, безусловно, могут существенно влиять на некоторые факторы поведенческих паттернов как в положительном, так и в отрицательном аспектах. Также отсутствуют факторы текущего состояния сотрудника, несмотря на их очевидную важность. Примерами таких факторов могут служить проблемы в личной жизни или недосып, которые, несомненно, могут влиять на поведение сотрудника. Однако, при анализе психологических характеристик целой группы такие показатели не стоит учитывать, из-за их неоднородности внутри группы.

Анализ отдельного сотрудника в сравнении с анализом целой группы может дать значительно разные результаты, но такой подход может привести к более точным выводам. Сбор информации о каждом сотруднике отдельно является более выполнимой задачей, и при детальном анализе есть возможность присваивать веса связям в модели. Это позволит модели быть более чувствительной к преобладающим факторам в личностных характеристиках. Дополнительные показатели, такие как проблемы в личной жизни, возраст и недосып, могут помочь дополнительно сформировать сценарии критических ситуаций. Все это в совокупности повысит точность и качество моделирования, что в конечном итоге повысит эффективность противодействия угрозам.

3. Заключение

В заключение следует отметить, что развитие технологий, в частности искусственного интеллекта, позволяет не только улучшить безопасность предприятий, но и дает возможность правонарушителям повысить эффективность атак в области информационной безопасности. В контексте фишинга и социальной инженерии в целом, ИИ может улучшить множество аспектов атак – персонализацию, адаптацию, реалистичность, скорость, подбор аудитории. Более того, следует подчеркнуть одну из ключевых проблем: всеобщее применение искусственного интеллекта позволяет снизить порог входа для злоумышленников. В то время как крупные корпорации могут тратить значительные средства на обеспечение информационной безопасности, обычным гражданам такие возможности недоступны. Появление новых видов атак требует постоянного обучения и внимательности, на что у большинства людей часто нет времени или ресурсов.

В работе не рассматриваются факторы, связанные с действиями внутренних нарушителей. Противодействие такого рода угрозам, в сравнении с внешними атаками, требует иных методов обнаружения и воздействия в связи с отличающимися целями, задачами и мотивацией таких сотрудников.

Литература

1. *Oechssler J., Roider A., Schmitz P. W.* Cognitive abilities and behavioral biases // Journal of Economic Behavior & Organization. – 2009. – Vol. 72. №. 1. – P. 147-152.
2. *Krekels G., Pandelaere M., Weijters B.* Dispositional greed: scale development and validation // ACR North American Advances. – Association for Consumer Research, 2011. – P. 799-800.
3. *Colquitt J. A., Scott B. A., LePine J. A.* Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance // Journal of Applied Psychology. – 2007. – Vol. 92. №. 4. – P. 909.
4. *Firestein S.* Ignorance: How it drives science. – OUP USA, 2012. – 195 p.
5. *Chernov I., Feyzov V.* Scenario Models Based on a Digital Portrait of a Person //2022 15th International Conference Management of large-scale system development (MLSD). – IEEE, 2022. – P. 1-5.
6. *Belch G. E.* Advertising and promotion: An integrated marketing communications perspective. – New York: McGraw-Hill/Irwin, 2004. – T. 6. – 864 p.
7. *He J., Wang C. L.* Cultural identity and consumer ethnocentrism impacts on preference and purchase of domestic versus import brands: An empirical study in China //Journal of Business Research. – 2015. – Vol. 68. №. 6. – P. 1225-1233.
8. *Luthans F., Youssef C. M., Avolio B. J.* Psychological capital: Developing the human competitive edge. – Oxford University Press, 2006. – 256 p.
9. *Bowie N. E.* The Blackwell guide to business ethics. – Wiley-Blackwell, 2002. – 376 p.
10. *Bohlander G., Snell S.* Managing Human Resources. – South-Western Cengage Learning, 2009. – 821 p.
11. *Armstrong M., Taylor S.* Armstrong's handbook of human resource management practice. – Kogan Page Publishers, 2020. – 776 p.
12. *Arvisais M. A.* Primal leadership: Realizing the power of emotional intelligence //Journal of Organizational Change Management. – 2003. – Vol. 16. №. 1. – P. 123-126.

13. *Melville N., Kraemer K., Gurbaxani V.* Information technology and organizational performance: An integrative model of IT business value // MIS quarterly. – 2004. – P. 283-322.
14. *DeMarco T., Lister T.* Waltzing with bears: Managing risk on software projects. – Addison-Wesley, 2013. – 196 p.
15. *Rao J. V., Chandraiah K.* Occupational stress, mental health and coping among information technology professionals // Indian journal of occupational and environmental medicine. – 2012. – Vol. 16. №. 1. – P. 22.