МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ВИНИТИ РАН)

НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

Издается с 1961 г. **№ 11** **Москва 2020**

ОБЩИЙ РАЗДЕЛ

УДК 005:004.056

Л.В. Астахова

Валидность методик оценки угроз информационной безопасности организации*

На основе статистических данных показано противоречие между увеличением финансовых вложений в информационную безопасность (ИБ) организаций и стабильным ростом угроз ИБ по вине внутренних пользователей. Сделан вывод о когнитивной уязвимости и низкой степени валидности современных методик оценки рисков ИБ. Выявлены стереотипы, следствием которых являются когнитивные ошибки оценивания рисков ИБ: приоритет технической защиты информации от внешних угроз ИБ над организационной и технической защитой от угроз внутренних; недоверие к внутреннему клиенту, восприятие его исключительно как объекта жесткого управленческого воздействия, игнорирование его субъектной роли в управлении ИБ; ограничение работы с персоналом в рамках системы управления ИБ разовыми мерами и статическими критериями оценки человеческих рисков и невнимание к системным мерам и динамическим, ситуационным критериям. Обосно-

* Статья подготовлена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г., соглашение № 02. А03.21.0011)

вана необходимость обновления стандартов по управлению угрозами ИБ, а также разработки новых методик и средств оценки этих угроз на условиях отказа от устаревших стереотипов.

Ключевые слова: *риск, информационная безопасность, методика, валидность, когнитивные искажения, когнитивные ошибки, внутренний нарушитель, человеческие угрозы, вовлеченность, ситуационная осведомленность*

DOI: 10.36535/0548-0019-2020-11-1

ВВЕДЕНИЕ

Человеческий капитал – это важнейший актив любой организации, поэтому он, как любой капитал, имеет свои уязвимости. Угрозы информационной безопасности со стороны человека (сотрудника, работника организации, внутреннего клиента, внутреннего нарушителя, пользователя информационной системы и др.) весьма опасны. Ежегодные аналитические отчеты, подготовленные зарубежными и российскими компаниями, свидетельствуют о стабильно непрерывном росте числа инцидентов угроз ИБ организаций, произошедших по вине внутренних нарушителей. Впервые с 2004 г. внутренние утечки информации показали более высокую «мощность», чем внешние: в результате одной внутренней утечки оказался скомпрометированным гораздо больший объем данных, чем в результате одной внешней [1]. По результатам исследований, 77% компаний считают внутренние инциденты более опасными, чем внешние. 16% российских компаний отметили рост числа внутренних инцидентов. Не менее 40% компаний в России и 30% в СНГ сталкивались с попытками уволенных сотрудников навредить компании. Виновниками угроз ИБ в 2019 г. в 27% случаев были руководители, в 73% – рядовые сотрудники. И это при том, что компании вкладывают в ИБ финансовые средства (64% компаний сообщили об отсутствии динамики в изменении бюджета на ИБ в 2019 г., а 25% – о его повышении) и работают над осведомленностью сотрудников в области ИБ (75% предприятий назвали ИБ-инструктаж в числе методов защиты, которые применяются в организации) [2].

Интересны результаты сравнительного анализа распределения утечек конфиденциальной информации в финансовом сегменте: если во всем мире в 2019 г. доля внутренних злоумышленников составляла 37,4%, то в России – 91,3%. В России произошло более чем в 2 раза больше утечек с целью мошенничества с использованием данных, по сравнению с другими странами мира (44,2% и 19,3% соответственно) [3].

Рост числа инцидентов угроз ИБ по вине внутренних клиентов при стабильном бюджетировании и мерах по повышению их осведомленности приводит нас к выводу о повышении опасности угроз со стороны человека, усилении их злоумышленного характера и, следовательно, – о важности эффективного управления ими. Низкая эффективность всех усилий по предотвращению угроз ИБ свидетельствует об углублении когнитивных искажений в процессе оценивания рисков ИБ и когнитивной уязвимости современных методик такой оценки, низкой степени их валидности.

Валидность отражает качество измерения параметров объектов, степень соответствия измеренного показателя тому, что подлежит измерению, и предполагает отсутствие исходных когнитивных ошибок на стадии разработки методики измерения.

Ошибки являются следствием когнитивного искажения свойств изучаемых объектов. *Когнитивное искажение* в понимании зарубежных ученых – это систематически повторяющееся эволюционно сформировавшееся отклонение в восприятии, поведении и мышлении, которое на ситуативном уровне обусловлено субъективным восприятием индивида, социальными, моральными и эмоциональными стереотипами, а также спецификой ограниченных возможностей человеческого мозга по приёму, переработке и репрезентации информации [4]. Когнитивные искажения влияют одновременно на восприятие, мышление и в особенности – на действия людей.

Мы выделяем три основных когнитивных искажения оценки угроз ИБ. Существующие методики отражают, во-первых, сосредоточенность на технических аспектах защиты от внешних атак и недостаточное внимание влиянию внутренних факторов (мотивации и поведения пользователей); во-вторых, – низкую степень использования их человеческого потенциала, отсутствие вовлеченности сотрудников в процесс управления угрозами ИБ; в-третьих, – проблемы реализации ситуационной, динамической оценки угроз ИБ. Рассмотрим их подробнее.

КОГНИТИВНОЕ ИСКАЖЕНИЕ ОЦЕНКИ УГРОЗ ИБ ВСЛЕДСТВИЕ НЕДОСТАТОЧНОГО ВНИМАНИЯ К ВНУТРЕННИМ, ЧЕЛОВЕЧЕСКИМ РИСКАМ

Организации в большей степени ориентированы на защиту от внешних атак и угроз для обеспечения конфиденциальности, целостности и доступности своих информационных активов, часто не учитывая внутренние угрозы.

Эта проблема в последнее время становится объектом специальных научных исследований. Так, зарубежные эксперты рассмотрели известные методики оценки угроз (метод OCTAVE Карнеги-Меллона, COBIT, ITIL, CORAS, ISRAM и CRAMM, а также другие, которые представлены и перечислены ENISA) [5]. Результаты этого и других исследований [6, 7] показывают низкую эффективность процессов управления информационной безопасностью. Авторы этих исследований демонстрируют, что предприятия, внедряющие широко используемые методы обеспечения безопасности, продолжают испытывать трудности с оценкой, управлением своими угрозами

и осуществлением соответствующих мер безопасности. Они приходят к выводу, что имеющиеся модели и структуры управления угрозами информационной безопасности в основном сосредоточены на технических аспектах и не уделяют большого внимания влиянию внутренних факторов (мотивации и поведения пользователей) на надежность принимаемых решений [8, 9].

Зарубежные исследователи активизировали изучение проблем предотвращения и обнаружения внутренних угроз в начале 2000-х гг. Так, они предложили основу для прогнозирования атак со стороны инсайдеров, в основном, на основе личностных качеств и словесного поведения [10]; использовали атрибуты метрик знаний, привилегий и навыков пользователей [11]; смоделировали инсайдерский профиль посредством идентификации атрибутов персонала, изучили связь между намерениями и действиями пользователя [12]; предложили метод измерения неправомерного использования инсайдерами стандарта ISO17799 [13] и др. Уже тогда появились разработки, в которых предпринимались попытки интеграции технических и психологических решений. Например, авторы [14] представили модель для предсказания поведения инсайдеров с помощью использования таксономии пользователя, психологического профилирования и алгоритма принятия решений для выявления потенциально опасных пользователей.

Справедливости ради заметим, что и в сугубо технических решениях встречаются оценки внутренних угроз. Так, системы обнаружения вторжений могут применяться для выявления внутренних нарушений политик безопасности, аномальной активности в информационной системе. Это может быть достигнуто с использованием технологий искусственного интеллекта [15]. Авторы [16] проиллюстрировали это на примере системы, которая моделирует жизненный цикл пользователя для анализа его взаимодействия с внутренними стратегиями защиты безопасности. Другие подходы основаны на производстве приманок для выявления потенциальных злоупотреблений со стороны инсайдеров.

Понятно, что конечными угрозами являются все же те, которые не оставляют технологически обнаруживаемый след в системе или не используют обычные действия для совершения злонамеренных действий. Поэтому требуются более широкие методы оценки угроз ИБ, связанных с персоналом. Этот факт учитывается в современных методиках и средствах оценки систем ИБ. Например, Microsoft Security Assessment Tool (MSAT) – это средство оценки угроз, предоставляющее информацию о системе безопасности ИТ-инфраструктуры и рекомендации по ее улучшению, основанные на передовом опыте. По словам разработчика, «данное средство использует целостный подход к оценке системы безопасности, анализируя влияние человеческого фактора, процессов и технологий» [17].

Оценка человеческого фактора базируется на следующих вопросах: существует ли в компании в отношении безопасности индивидуальная или групповая ответственность; обладает ли лицо или группа лиц должным опытом в области безопасности; участвует ли это лицо или группа в определении требований по безопасности для новых и существующих технологий; на каких стадиях жизненного цикла технологий привлекается данное лицо или группа, обеспечивающая безопасность (планирование и проектирование, реализация, тестирование, развертывание); определены ли роли и обязанности для каждого лица, связанного с информационной безопасностью; используются ли независимые сторонние специалисты для оценки безопасности среды; выполняют ли оценку безопасности среды внутренние специалисты организации; практикуются ли в организации проверки в фоновом режиме, являющиеся составной частью процесса найма; существует ли официальная политика в отношении служащих, покидающих компанию; имеется ли официальная политика регулирования сторонних взаимосвязей; есть ли в компании программа уведомления о вопросах безопасности; проводится ли тематическое обучение для служащих в зависимости от их роли в организации. Предлагаемые разработчиками этого средства [17] вопросы и рекомендации основаны на существующих стандартах (ISO/IEC 17799-2005 Technologies de l'information – Techniques de security – Code de pratique pour la gestion de security d'information. Информационная технология – Методы защиты – Практическое руководство для менеджмента информационной безопасности (п.8. Безопасность человеческих ресурсов) [18] и NIST-800.x NIST (National Institute of Standards and Technology – Американский национальный институт стандартизации) (Раздел «Создание программы повышения осведомленности в области безопасности ИТ») [17, 19, 20,]. К сожалению, они не учитывают психологические аспекты поведения внутренних клиентов, а потому носят ограниченный характер.

К такому же выводу приходят и другие эксперты, утверждая, что, несмотря на то, что существует значительное количество моделей, предназначенных для устранения внутренних угроз, они, как правило, решают проблему лишь ограниченно, уделяя особое внимание отдельным выделенным метрикам, которые очень трудно интегрировать в единый подход к оценке угроз [14, 21].

Российские ученые также обратили внимание на угрозы неконтролируемых, игнорируемых внутренних уязвимостей. Так, А.А.Кононов для решения этой проблемы предлагает методологию детального критериального моделирования, включающую целый ряд методов, комплексное использование которых позволяет в значительной степени снять проблемы, связанные с охватом и оценкой опасности всего множества возможных уязвимостей, как бы велико оно ни было [22]. Поэтому все больше экспертов обсуждают методологические проблемы для оценки внутренних угроз и их последствий, а также – их интегрирования в структуру угроз безопасности, которая была определена в соответствии со стандартами безопасности серии ISO / IEC 27000 по управлению ИБ [5].

Возможность задавать сценарии внутренних угроз может быть полезным средством снижения. Авторы [23] разработали модели инсайдерских угроз, которые помогают количественно оценивать угрозы

и определять меру вероятности возникновения конкретных сценариев их реализации.

Таким образом становится понятно, что для оценки внутренних угроз ИБ первоочередными задачами работодателя являются: оценка предрасположенности пользователя к злонамеренному поведению и его ИТ-навыков; разработка процедур сбора информации о восприятии пользователями, отношении и чувствах, поведении в отношении безопасности и связанных с ними рисках; создание показателей измерения. При этом все приведенные действия должны быть документированы в международных и национальных стандартах по ИБ, используемых для сертификации организаций [5], в документах государственных регуляторов, обязательных для исполнения. Достаточно сказать, что в других сферах такие стандарты существуют [24, 25].

КОГНИТИВНОЕ ИСКАЖЕНИЕ ОЦЕНКИ УГРОЗ ИБ ВСЛЕДСТВИЕ НЕВОВЛЕЧЕННОСТИ СОТРУДНИКОВ В ПРОЦЕСС УПРАВЛЕНИЯ ИМИ

В последние годы в теории управления особо пристальное внимание уделяется вовлечению сотрудников организации – их готовности целиком вкладывать когнитивную, эмоциональную и физическую энергию в работу [26–28]. В во всех сферах когнитивного общества человек стал полноправным субъектом информационной деятельности. Однако в сфере защиты информации сложилась устойчивая практика дистанцирования работодателя от сотрудников, которые во всех существующих методиках оценки угроз остаются пассивными объектами управленческих воздействий. Гипертрофированный контроль за сотрудниками организации со стороны руководства неизбежно ведёт к негативным психологическим последствиям: стрессы, озлобленность, утрата доверия к руководству и другие причины и обстоятельства, которые, как правило, приводят не к ожидаемому снижению, а, напротив, – к повышению их уязвимости в системе защиты информации. В условиях взаимного недоверия работодатель рано или поздно теряет своих даже очень лояльных сотрудников. В других сферах деятельности давно осознана критическая важность доверительного фактора. Так, в атомной энергетике есть принцип "организация пронизана доверием" для достижения культуры ядерной безопасности. Атмосфера доверия в организации складывается из осознанного отношения рабочей среды к вопросам безопасности (SCWE – safety-conscious work environment – рабочая обстановка с сознательным отношением к вопросам безопасности) и уважения между руководителями и персоналом, когда в действиях и решениях руководства отсутствуют признаки "сковывающего эффекта", преследования, запугивания, мести или дискриминации сотрудников [29].

Сфера информационной безопасности остро нуждается в повышении доверия между работодателем и сотрудниками организации. В одном из своих исследований мы определили онтологический статус доверия в информационной безопасности следующим образом: «доверие в информационной безопасности – это *информационно-измерительный механизм управления* (планирования, реализации, контроля и мотивации) безопасным взаимодействием субъектов информационных отношений, направленным на их устойчивое функционирование и развитие» [30]. Акцент на сотрудниках организации как субъектах информационных отношений, их потребностях в защищенности и развитии, степени гармонизации их информационного взаимодействия с работодателями, их информационно-психологической безопасности, безусловно, позволяет измерить степень их лояльности к организации. Позитивные, взаимнодоверительные отношения руководителя и сотрудников более эффективны для обеспечения информационной безопасности.

Ярким примером нашего концептуального подхода к статусу доверия к ИБ является концепция человека как датчика (сенсора) безопасности (The Human-as-a-Security-Sensor paradigm), которая активно развивается сегодня в зарубежной науке и практике. Зарубежные эксперты уверены в том, что сотрудники могут быть уполномочены брать на себя ответственность за информационную безопасность организации [31], могут быть «последней линией защиты» [32], они разрабатывают специальные продукты для того, чтобы пользователи имели возможность самостоятельно обнаруживать социоинженерные атаки и сообщать о них в соответствующие подразделения организации [33]. Это значит, что доверительное делегирование и расширение прав и возможностей сотрудников в области управления ИБ вполне может и должно быть включено как в стандарты по управлению угрозами ИБ, так и в структуру показателей в методиках оценки этих угроз.

КОГНИТИВНОЕ ИСКАЖЕНИЕ ОЦЕНКИ УГРОЗ ИБ ВСЛЕДСТВИЕ РЕАЛИЗАЦИИ ДИНАМИЧЕСКОЙ, СИТУАЦИОННОЙ ИХ ОЦЕНКИ

Стандартом National Institute of Standards and Technology NIST SP 800-53 rev.5 Security and Privacy Controls for Information Systems and Organizations («Меры обеспечения безопасности и конфиденциальности для информационных систем и организаций», редакция 5, март 2020) [19] предусмотрена актуализация оценки угроз с использованием результатов непрерывного их мониторинга (Раздел 3.16 RISK ASSESSMENT). В приложениях к данному стандарту содержатся примеры расчетов по каждой из подзадач, а также перечни возможных источников угроз, событий угроз, уязвимостей и предварительных условий. NIST SP 800-137 rev. 2 Information Security Continuous Monitoring for Federal information Systems and Organizations («Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций», редакция 2, декабрь 2018) [20] описывают стратегию непрерывного мониторинга информационной безопасности. Цель её построения – оценка эффективности мер защиты и статуса безопасности систем для реагирования на постоянно меняющиеся вызовы и задачи в сфере информационной

безопасности. Непрерывный мониторинг ИБ помогает предоставлять ситуационную осведомленность о состоянии безопасности информационных систем компании на основании данных, собранных из различных ресурсов (таких как активы, процессы, технологии, сотрудники), а также сведений об имеющихся возможностях по реагированию на изменения ситуации [34].

Однако эксперты указывают, что выявленные методы комплексной оценки угроз для защиты и безопасности по-прежнему для динамической оценки рисков не учитывают системную информацию, которая необходима, чтобы сделать эту оценку более эффективной [35].

Обоснованные когнитивные искажения оценки угроз ИБ вызваны объективно сложившимися стереотипами. Бурный рост технологического прогресса и развитие средств информатизации и связи в XX в. были акцентированы на технической защите информации. Условия «холодной войны» вполне объясняют приоритеты внешних угроз ИБ. Невнимание к внутренним угрозам ИБ в большой степени обусловлено опытом режимной защиты государственной тайны и эффективной советской системой воспитания, высокоразвитыми патриотическими и морально-нравственными ценностями граждан. Трудности формализации процессов оценки психологических аспектов деятельности человека не позволили включить человеческие критерии в стандарты и методики оценки угроз ИБ. Наконец, отсутствие технологических основ мониторинга уровня ИБ организации объясняют невнимание к ситуационному управлению человеческими угрозами ее безопасности.

Как видим, названные когнитивные искажения в оценивании угроз ИБ носят вполне объективно-детерминированный характер. Теоретические исследования также показывают, что «искажение является неотъемлемой частью процесса познания окружающей, текучей и мерцающей реальности, отражая особенности приспособления субъекта к этим процессам» [36, с. 68], это «часть природы познавательных механизмов, им априори подвержены все субъекты» [36, с. 67]. Однако «искажение может быть субъективным, отображать уникальность внутрипсихических процессов индивида, обусловленных ситуативными факторами» [36, с. 67]. По словам экспертов в области когнитивных искажений, мы не можем «рационализировать» то, что нерационально с самого начала – как если бы ложь называли истиной… Можно заставить больше людей поверить в то или иное суждение, но невозможно сделать его более истинным. Чтобы усилить истинность убеждений, мы должны изменить эти убеждения [37], проверив их на практике.

Поэтому полагаем, что гораздо более эвристично для практики управления угрозами ИБ понятие когнитивной ошибки. В отличие от когнитивных искажений, когнитивные ошибки обладают важной характеристикой верифицируемости и обеспечивают качество прогноза развития ситуации и результативности деятельности: предполагают наличие точных данных о том, *какое решение следовало принять и к каким последствиям привело использование той или иной когнитивной схемы*. Например, врач, поставивший неверный диагноз, т.е. совершивший врачебную ошибку, может признать этот факт при ухудшении состояния больного. Иными словами, «ошибка помещает человека в условия верифицируемые, подверженные проверке и нахождению верных ответов на вызовы действительности» [36]. Найти верные ответы на рост внутренних угроз и уязвимостей – это как раз то, в чем нуждается сегодня сфера управления угрозами ИБ.

Данное утверждение позволяет заключить, что новой угрозой ИБ являются когнитивные ошибки в результатах оценки рисков ИБ организаций на основе современных методик, которые разработаны на основе описанных в настоящей статье стереотипов. Об этих ошибках свидетельствует устойчивый рост числа инцидентов угрозы ИБ, связанных с внутренними нарушителями организаций, даже если они практикуют использование оценки этих угроз. Реализация представленных методик не позволяет избежать ущерба от растущего числа инцидентов угрозы ИБ. Признание факта ошибок требует поиска более верных ответов на вопрос, как оценивать эти угрозы. Очевиден вывод о необходимости включения в методики оценки угроз формализованных и неформализованных методов мониторинга и обработки человеческих угроз и учета степени вовлеченности внутренних клиентов в процессы управления информационной безопасностью и доверия к ним.

Позитивным фактом признания когнитивных искажений и ошибок оценки угроз ИБ становится появление на современном рынке защиты информации инструментов, которые способны осуществлять мониторинг данных о действиях сотрудника на рабочем месте. Так, InfoWatch Person Monitor – это простой и быстрый способ выявлять нелояльных сотрудников и контролировать действия привилегированных пользователей. Собирать полную информацию о действиях пользователя позволяют: запись скриншотов и видео с экрана, изображения с веб-камеры, звук с микрофона и динамиков; входящие и исходящие сообщения электронной почты, вложенные файлы; мониторинг коммуникаций в мессенджерах Lync, Skype, Teams, Viber, Telegram, WhatsApp, Bitrix24 и т.д.; посещаемые сайты и интернет-запросы, передача файлов через файлообменники, веб-почту и чаты; статистика использования приложений и мониторинг вводимого текста; распознавание лиц с веб-камер для контроля присутствия и идентификации сотрудников; операции с документами: удаление, печать, копирование на внешние носители и в облако; факт присутствия на рабочем месте и в офисе, время, проведенное за компьютером; геолокация мобильных устройств и ноутбуков на платформах Android, Windows 10; расширение возможностей мониторинга на ПК под управлением MacOS и Astra Linux. Эти меры позволят службе ИБ взять под контроль управление человеческими угрозами информационной безопасности [38].

ProfileCenter – еще одно программное решение, которое применяется для выявления мошеннических действий, прогнозирования и обнаружения деструктивного поведения сотрудников в отношении организации, а также позволяет просчитывать угро-

зы личности для окружающих или компании. ProfileCenter готов предоставить актуальную и развернутую характеристику на каждого сотрудника, выявить значимые колебания настроений работников, а также оценить психологическую атмосферу в коллективе в любой момент. DLP-система собирает переписку сотрудника: исходящие письма, сообщения в Skype, Viber, WhatsApp, Lync, Telegram, других мессенджерах и социальных сетях. В любой момент с помощью этой системы можно увидеть потенциальные угрозы, связанные с конкретным сотрудником, и рекомендации по их снижению: за кем из сотрудников необходимо следить время от времени, а за кем – постоянно или в определенных ситуациях; подходит или нет сотрудник на ту или иную должность, обладает ли нужными качествами и т.д.; насколько безопасно давать сотруднику доступ к конфиденциальной информации, финансовым активам и ценным ресурсам компании; с кем в коллективе можно сохранять подчеркнуто деловые, формальные отношения, а с кем, наоборот, наладить дружеские связи; кому из сотрудников достаточно «внушения» и профилактической беседы, а с кем следует регулярно проводить тренинги по информационной безопасности; кого следует более строго наказывать за нарушение правил и т.д. [39]. Разработка и использование новых подобных методик и средств оценки, их интегрирование в существующие методики и средства, а также обновление стандартов по управлению угрозами ИБ и принятие специальных стандартов по управлению человеческими угрозами ИБ – вот реакция, которая должна последовать за признанием когнитивных искажений и ошибок в оценивании угроз ИБ.

В организациях целесообразна разработка локальных документов по управлению угрозами ИБ, в которых следует предусматривать требование использовать методики оценки угроз, которая разработана на основе стратегии триангуляции – комбинирования не менее 3-х количественных и качественных методов измерения. Изучение валидизирующей функции триангуляции в методологии является значимым трендом в современных социальных науках и психологии [40]. Основываясь на совокупности разных типов триангуляции [41], логично заключить, что для повышения достоверности результатов оценки угроз ИБ следует учитывать: не только статические, но и динамические показатели угроз, изменения во времени и пространстве (триангуляция данных); оценочные мнения руководителей разных структурных подразделений как разных субъектов оценки угроз ИБ (триангуляция исследователей); не только теорию инженерно-технической защиты информационных систем, но и теорию организационно-технического обеспечения ИБ, связанной с персоналом (триангуляция теорий); данные, полученные с помощью самых разных методов: анализа статистики об источниках и видах инцидентов угрозы ИБ в организации; данных о свойствах источников рисков, полученных с помощью наблюдения, вопросников, инструментального мониторинга, экспертных оценок, степени вовлеченности персонала в управление ИБ и др. (методологическая триангуляция). Только наличие устойчивой корреляции между результатами, полученными с помощью разных подходов в рамках такой интегративной методики, может служить одним из оснований для признания этой методики валидной. В условиях развития технологий машинного обучения следует предположить необходимость и возможность создания инструментальных средств оценки угроз ИБ, положив в их основу интегративные методики, которые были представлены в настоящей статье.

ЗАКЛЮЧЕНИЕ

Управление угрозами информационной безопасности сегодня практикуется в большинстве организаций, однако число угроз по вине внутренних пользователей неуклонно растет. Это свидетельствует о том, что существующие методики оценки угроз ИБ и созданные на их основе средства несовершенны, т.е. обладают когнитивной уязвимостью. Оценивание рисков согласно этим методикам основано на отклонениях в восприятии, поведении и мышлении, на ошибочных стереотипах: 1) о приоритете технической защиты информации от внешних угроз ИБ; 2) о внутреннем клиенте исключительно как об объекте жесткого управленческого воздействия, отрицая его субъектную роль в управлении ИБ; 3) о достаточности работы с персоналом в рамках системы управления ИБ и о невозможности учета ситуационных критериев оценки. Эти стереотипы не только приводят к ошибочным результатам оценки угроз ИБ, но и препятствуют гармонизации отношений работодателя и работников или приводят к разрушению их взаимного доверия, усиливая уязвимость организации. Поэтому процессы оценки угроз ИБ на основе существующих методик представляют собой когнитивное искажение, а результаты этих процессов – когнитивные ошибки, являющиеся новыми угрозами информационной безопасности в эпоху трансформации культуры и социальных ролей в обществе знания. Для исправления этих ошибок необходим отказ от показанных в настоящей статье стереотипов и разработка принципиально новых практик работы с внутренними клиентами, методик и средств оценки человеческих угроз ИБ. Важнейшей задачей становится обновление стандартов по управлению угрозами информационной безопасности, принятие специальных стандартов по управлению человеческими угрозами, разработка интегративных методик оценки угроз информационной безопасности и создание на их основе новых инструментальных средств.

СПИСОК ЛИТЕРАТУРЫ

1. PriceWaterhouseCoopers. The Global State of Information Security® Survey 2018. – URL: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html (дата обращения 31.03.2020).
2. Исследование уровня информационной безопасности в компаниях России и СНГ за 2019 год. – URL: https://searchinform.ru/research-2019/ (дата обращения 31.03.2020).

3. Исследование утечек конфиденциальной информации из организаций финансового сегмента в 2019 г. – URL: https://www.infowatch.ru/analytics/reports/21649 (дата обращения 31.03.2020).
4. Канеман Д., Словик П., Тверски А. Принятие решений в неопределенности: Правила и предубеждения. – Харьков: Изд-во Института прикладной психологии «Гуманитарный Центр», 2005. – 632 с.
5. Pereira T., Santos H. Insider Threats: The Major Challenge to Security Risk Management // Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science / eds T. Tryfonas, I. Askoxylakis. – 2015. – Vol. 9190. – P. 654-663.
6. Sadok M., Spagnoletti P. A business aware information security risk and analysis method // Information Technology and Innovation treads in Organization / eds. A. D'Atri, M. Ferrara, J.F. George, P. Spagnoletti. – 2011. – P. 453–460.
7. Asosheh A., Dehmoubed B., Khani A. A new quantitative approach for information security risk assessment // IEEE International Conference on Intelligence and Security Informatics. (ISI 2009), – 2009 8–11 June. – P. 229–239. – URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5137311&isnumber=5137253. DOI: 10.1109/ISI.2009.5137311 (дата обращения 31.03.2020).
8. Posey C., Roberts T.L., Lowry P.B., Bennett R.J., Courtney J. Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors // MIS Q. – 2013. – Vol. 37(4). – P. 1189–1210.
9. Posey C., Roberts T.L., Lowry P.B., Hightower R.T. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders // Inf. Manag. – 2014. – Vol. 51(5). – P. 551–567. – URL: http://dx.doi.org/CrossRefGoogle Scholar (дата обращения 31.03.2020)].
10. Schultz E.E. A framework for understanding and predicting insider attacks. // Comput. Secur. – 2002. – Vol. 21(6). – P. 526–531.
11. Wood B. An insider threat model for adversary simulation // Research on Mitigating the Insider Threat to Information Systems. RAND / ed. R.H. Anderson. – 2000. – №2. – URL: https://www.yumpu.com/en/document/read/22015185/an-insider-threat-model-for-adversary-simulation- (дата обращения 01.04.2020).
12. Caputo D., Marcus A., Maloof M., Stephens G. Detecting insider theft of trade secrets // IEEE Secur. Priv. – 2009. – Vol. 7(6). – P. 14–21.
13. Theoharidou M., Kokolakis S., Karyda M., Kiountouzis E. The insider threat to information systems and the effectiveness of ISO17799 // Comput. Secur. – 2005. – Vol. 24(6). – P. 472–484.
14. Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D. An insider threat prediction model // Business.TrustBus. Lecture Notes in Computer Science / eds. S. Katsikas, J. Lopez, M. Soriano. – 2010. – Vol. 6264. – P. 26–37. – https://doi.org/10.1007/978-3-642-15152-1_3
15. Cappelli D.M., Moore A.P., Trzeciak R.F., Shimeall T.J. Common Sense Guide to Prevention and Detection of Insider Threat, 3rd edn. – Pittsburgh: Carnegie Mellon University, 2009.
16. Duran F., Conrad S., Conrad G., Duggan D., Held E. Building a system for insider security // IEEE Secur. Priv. – 2009. – Vol. 7(6). – P. 30–38.
17. Средство Microsoft Security Assessment Tool 4.0. – URL: https://www.microsoft.com/ ru-RU/download/details.aspx?id=12273 (дата обращения 31.03.2020).
18. ISO/IEC 17799-2005 Technologies de l'information – Techniques de security – Code de pratique pour la gestion de security d'information. [Информационная технология – Методы защиты – Практическое руководство для менеджмента информационной безопасности]. –URL: https://www.iso.org/standard/39612.html (дата обращения 31.03.2020).
19. NIST SP 800-53 rev.5 Security and Privacy Controls for Information Systems and Organizations. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf (дата обращения 31.03.2020).
20. NIST SP 800-137 Information Security Continuous Monitoring for Federal information Systems and Organizations. – URL: https://nvlpubs.nist.gov/ nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. (дата обращения 31.03.2020).
21. Beres Y., Mont M.C., Griffin J., Shiu S. Using security metrics coupled with predictive modeling and simulation to assess security processes // 3rd International Symposium on Empirical Software Engineering and Measurement, Lake Buena Vista, FL, USA, 2009. – P. 564–573. DOI:10.1109/ESEM.2009.5314213
22. Кононов А.А. Когнитивные искажения как угрозы информационной безопасности и методы их парирования // Современные проблемы и задачи обеспечения информационной безопасности: сб. статей. – Москва, 2017. – С. 27-32.
23. Coles-Kemp L., Theoharidou M. Insider Threat and Information Security Management // Insider Threats in Cyber Security. Advances in Information Security / eds. C. Probst, J. Hunker, D. Gollmann, M. Bishop. – Boston, MA: Springer, 2010. – Vol 49. – P. 45-71.
24. ГОСТ Р 22.3.07-2014 Безопасность в чрезвычайных ситуациях. Культура безопасности жизнедеятельности. Общие положения. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 11 марта 2014 г. N 107-ст. – URL: https://base.garant.ru/70981162/ (дата обращения 31.03.2020).
25. ГОСТ Р МЭК 62508-2014 Менеджмент риска. Анализ влияния на надежность человеческого фактора. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17 октября 2014 г. N 1350-ст. – URL: https://base.garant.ru/71268248/ (дата обращения 31.03.2020).

26. Saks A.M. Translating Employee Engagement Research into Practice // Organizational Dynamics. – 2017. – Vol. 46, Issue 2(April–June). – P. 76-86.
27. Employee engagement and motivation. Understand the concept of employee engagement and learn how to build an engaged and motivated workforce / Chartered Institute of Personnel and Development. – 2018. – URL: https://www.cipd.co.uk/ (дата обращения 31.03.2020).
28. Веретковская О.В. Вовлеченность персонала организации как актуальная задача современных компаний // Экономика и бизнес: теория и практика. – 2019. – № 4-2. – С. 40-43.
29. Машин В.А. Культура безопасности: принцип атмосферы доверия в организации // Электрические станции. – 2018. – № 9(1046). – С. 2-14.
30. Астахова Л.В. Онтологический статус доверия в информационной безопасности Научно-техническая информация. Сер. 1. – 2016. – № 3. – С. 1-9; Astakhova L.V. The ontological status of trust in information security // Scientific and Technical Information Processing. – 2016. – Vol. 43, №1. – P. 58-65.
31. Ashenden D., Sasse A. CISOs and organisational culture: Their own worst enemy? // Computers & Security. – 2013. – Vol.39, Part B. – P. 396-405.
32. Mansfield-Devine S. Raising awareness: people are your last line of defence // Computer Fraud & Security. – 2017. – Vol. 2017, Issue 11. – P. 10-14.
33. Heartfield R., Loukas G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework // Computers & Security. – 2018. – Vol. 76. – P.101-127.
34. Рахметов Р. Управление рисками информационной безопасности. Часть 5. Стандарт NIST SP 800-30 (продолжение). Стандарт NIST SP 800-137 – URL: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-5-standart-nist-sp-800-30-prodolzhenie-standar/(дата обращения 31.03.2020).
35. Chockalingam S., Hadžiosmanović D., Pieters W., Teixeira A., van Gelder P. Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications // Critical Information Infrastructures Security. CRITIS 2016. Lecture Notes in Computer Science / eds. G. Havarneanu, R. Setola, H. Nassopoulos, S. Wolthusen. – 2017. – Vol 10242. – P. 50-62.
36. Легостаева Е.С. Методологические предпосылки исследования когнитивных ошибок // Современная наука в теории и практике: моногр. / науч. ред. С.П. Акутина. –Москва, 2018. – С. 53-72.
37. Yudkowsky E. Cognitive Biases Potentially Affecting Judgment of Global Risks // Global Catastrophic Risks, edited by Nick Bostrom and Milan M. Ćirković. – New York: Oxford University Press, 2008. – P.91–119. – URL: https://intelligence.org/files/CognitiveBiases.pdf (дата обращения 01.04.2020).
38. Infowatch Person Monitor. – URL: https://www.infowatch.ru/products/person-monitor (дата обращения 31.03.2020).
39. СЁРЧИНФОРМ PROFILECENTER. – URL: https://searchinform.ru/products/kib/profilecenter (дата обращения 31.03.2020).
40. Мельникова О.Т., Хорошилов Д.А. Стратегии валидизации качественных исследований в психологии // Психологические исследования. – 2015. – Т. 8, № 44. – С. 3. – URL: http://psystudy.ru (дата обращения 18.04.2020).
41. Denzin N. The Research Act: A Theoretical Introduction to Sociological Methods. – New York: Imprint Routledge, 2009. – 379 p. – URL: https://doi.org/10.4324/9781315134543 (дата обращения 18.04.2020).

Материал поступил в редакцию 18.04.20.

Сведения об авторе

АСТАХОВА Людмила Викторовна – доктор педагогических наук, профессор, профессор кафедры защиты информации Южно-Уральского государственного университета (национального исследовательского университета), г. Челябинск
e-mail: astakhovalv@susu.ru