DOI: 10.24412/2070-1381-2022-91-226-241

Утечки конфиденциальных данных: главный враг внутри

Швыряев Павел Сергеевич
Аспирант, факультет государственного управления, МГУ имени М.В. Ломоносова, Москва, РФ.
E-mail: ShvyryaevPS@spa.msu.ru
SPIN-код РИНЦ: 6531-8970

Аннотация
Статья посвящена исследованию трендов в области утечек конфиденциальных данных в мире и России и социальных оснований данной проблемы. На базе анализа общемировых и российских аналитических отчетов выделяются наиболее важные тренды и проблемы: сохраняющийся высокий уровень количества утечек по всему миру; значительный рост доли внешних нарушителей, активизировавшихся во время вынужденной удаленной работы; главную угрозу с точки зрения объемов и ценности компрометируемых данных представляют сами сотрудники организаций, а не внешние нарушители; с точки зрения потенциальной угрозы компрометации данных особую опасность представляют увольняющиеся сотрудники. Отдельно проанализированы проблемы, ярко выраженные именно в России: замалчивание фактов утечек конфиденциальных данных от СМИ и общественности; нежелание или неготовность инвестировать ресурсы в развитие у сотрудников компетенций в области цифровой грамотности; непонимание необходимости или неготовность наращивать инвестиции в профилактику киберугроз, ликвидация последствий инцидентов уже по факту их свершения; высокий уровень уязвимости населения к утечкам персональных данных; несовершенство российской нормативно-правовой базы. В результате делается вывод о том, что все эти проблемы свидетельствуют о глобальной неподготовленности, непонимании глубинных основ происходящих цифровых трансформационных процессов, их рисков и потенциальных угроз; об отсутствии системного, стратегического подхода к реализации технологических преобразований. Поворот к иному пониманию происходящих сегодня цифровых процессов означает изменения не только в технологической, но и прежде всего в социальной сфере. Сложившаяся ситуация, системная по своей природе, требует системного подхода к своему разрешению для перехода к устойчивому цифровому развитию всего социума.

Ключевые слова
Конфиденциальная информация, персональные данные, утечка данных, киберпреступность, концепция нулевого доверия, устойчивое цифровое развитие.

Data Breaches: The Main Enemy Within

Pavel S. Shvyriaev
Postgraduate student, School of Public Administration, Lomonosov Moscow State University, Moscow, Russian Federation.
E-mail: ShvyryaevPS@spa.msu.ru

Abstract
The article is devoted to the study of trends in the field of data breaches in the world and in Russia and the social foundation for this problem. Based on the analysis of global and Russian analytical reports, the most important trends and problems are identified: the continued high level of the number of breaches around the world; a significant increase in the share of external security violators during remote work; the main threat in terms of the volume and value of compromised data is posed by the employees of the organizations themselves, and not by external violators; from the point of view of the potential threat of data compromise, leaving employees are especially dangerous. The problems that are clearly expressed in Russia are analyzed separately: suppression of the facts of data breaches from the media and the public; misunderstanding or unwillingness to invest resources in the development of digital literacy competencies in employees; lack of understanding or unwillingness to increase investments in the prevention of cyber threats, elimination of the consequences of incidents already after their occurrence; high level of vulnerability of the population to data breaches; imperfection of the Russian regulatory framework. As a result, it is concluded that all these problems indicate global unpreparedness, misunderstanding and lack of awareness of the deep foundations for the ongoing digital transformation processes, their risks and potential threats; lack of a systematic, strategic approach to the implementation of technological transformations. A turn to a different understanding of the digital processes means changes not only in the technological, but above all in the social sphere. The current situation, systemic in nature, requires a systematic approach to its resolution, as a turn towards sustainable digital development of the entire society.

Keywords
Confidential information, personal data, data breach, cybercrime, zero trust security model, sustainable digital development.

Введение

В 2017 г. журнал The Economist назвал данные самым ценным ресурсом в мире[1]. За последние годы резко возросло количество данных о действиях пользователей в сети, которые называют цифровым следом [Stier et al. 2020, 503]. Современный человек ежедневно

[1] The world's most valuable resource is no longer oil, but data // The Economist [Электронный ресурс]. URL: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (дата обращения: 26.10.2021).

оставляет большое количество информации о себе: деятельность в соцсетях, оплата покупок и заказ товаров, данные своих документов, поиск информации в Интернете, различный контент в виде текста, фото или видео, конфиденциальные данные по рабочей и учебной деятельности. Большие данные повсюду, и они не имеют определенного происхождения [Bayan et al. 2018, 1], однако представляют огромную ценность, поскольку содержат важную информацию о поведении людей или корпоративную тайну. Сегодня вокруг конфиденциальных данных возникает большое количество вопросов и проблем: использование в политических[2] и государственных[3] интересах, в качестве нечестного конкурентного преимущества[4]; проблемы в законодательстве в области защиты и использования персональных данных[5]; постоянные утечки в открытый доступ. Данная проблема становится все более актуальной частью жизни потребителей, а от возможной кибератаки не застраховано ни одно учреждение [Marcus 2018, 555]. Глобальный анализ утечек конфиденциальных данных организаций с 2005 по 2018 гг. показал, что наиболее подверженными инцидентам являются медицинские и бизнес-учреждения [Hammouchi et al. 2019, 1007].

Проблема утечек конфиденциальных данных организаций актуальна и для России. За последние годы произошли утечки данных клиентов «Сбера», «Альфа-банка», «Совкомбанка», «Вымпелкома»[6]. Серия громких событий с утечками данных в банковской сфере легко объяснима: в секторе финансовых услуг концентрируется большое количество конфиденциальной личной информации, что создает угрозы утечек данных [Сергеева, Али 2021, 25]. Проблема утечек также характерна и для государственной цифровой среды [Перекрестова, Фурсова 2021, 174]. Например, в сети оказывались данные российских автомобилистов, чиновников или москвичей, переболевших COVID-19[7]. На проблему защиты и пресечения незаконной деятельности в области конфиденциальных данных в последнее время регулярно обращает внимание и президент России Владимир Путин[8].

Одна из наиболее серьезных проблем, связанных с утечками данных, — это их использование в преступной деятельности. В России особую эффективность показывают мошеннические действия с использованием методов социальной инженерии на основании данных потенциальной жертвы[9].

---

[2] Скандал с Facebook и Cambridge Analytica. Что мы знаем // BBC [Электронный ресурс]. URL: https://www.bbc.com/russian/features-43475612 (дата обращения: 24.10.2021).

[3] Цифровая диктатура: как в Китае вводят систему социального рейтинга // РБК [Электронный ресурс]. URL: https://www.rbc.ru/business/11/12/2016/584953bb9a79477c8a7c08a7 (дата обращения: 26.10.2021).

[4] Каждый второй случай кражи корпоративной информации сотрудником при увольнении из организации связан с передачей этих данных конкурентам // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/company/presscenter/news/20590 (дата обращения: 30.11.2021).

[5] «Утечки неизбежны»: кто ответственен за персональные данные // Газета.ru [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2019/08/09_a_12567469.shtml (дата обращения: 26.10.2021); Приоткрытая информация: российские компании скрывают 57% утечек данных // Известия [Электронный ресурс]. URL: https://iz.ru/1121170/roman-kildiushkin/priotkrytaia-informatciia-rossiiskie-kompanii-skryvaiut-57-utechek-dannykh (дата обращения: 30.11.2021).

[6] Клиенты Сбербанка попали на черный рынок // Коммерсантъ [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4111863?from=main_1 (дата обращения: 24.10.2021); Данные клиентов Альфа-банка утекли в Сеть // РБК [Электронный ресурс]. URL: https://www.rbc.ru/finances/05/11/2019/5dbc07929a7947c6597cf70f?from=from_main (дата обращения: 24.10.2021); В Сеть попали данные желающих взять кредит в Совкомбанке // РБК [Электронный ресурс]. URL: https://www.rbc.ru/finances/24/09/2021/614db7e99a7947bd14dc2eb9 (дата обращения: 24.10.2021); Абонентов загрузили на сервер // Коммерсантъ [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4986542 (дата обращения: 24.10.2021).

[7] В открытом доступе оказалась база данных российских автовладельцев // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2020/05/14/830287-baza-avtovladeltsev (дата обращения: 24.10.2021); Паспортные данные российских чиновников попали в открытый доступ // Lenta.ru [Электронный ресурс]. URL: https://lenta.ru/news/2019/05/15/pass_open/ (дата обращения: 24.10.2021); «Ситуация критическая»: чем грозит крупнейшая утечка данных заболевших коронавирусом // Forbes [Электронный ресурс]. URL: https://www.forbes.ru/tehnologii/415857-situaciya-vesma-kritichna-chem-grozit-krupneyshaya-utechka-dannyh-zabolevshih (дата обращения: 30.11.2021).

[8] Путин призвал исключить утечки персональных данных при внедрении ИИ // Известия [Электронный ресурс]. URL: https://iz.ru/1095913/2020-12-04/putin-prizval-iskliuchit-utechki-personalnykh-dannykh-pri-vnedrenii-ii (дата обращения: 26.10.2021); Путин в 10 раз увеличил штрафы за разглашение персональных данных // РБК [Электронный ресурс]. URL: https://www.rbc.ru/rbcfreenews/60c386559a7947633c35d10d (дата обращения: 26.10.2021).

[9] Зампред Банка России Герман Зубарев: как победить телефонных мошенников // Российская газета [Электронный ресурс]. URL: https://rg.ru/2021/10/26/zampred-banka-rossii-german-zubarev-kak-pobedit-telefonnyh-moshennikov.html (дата обращения: 27.10.2021).

Мошенник, представляясь сотрудником банка или правоохранительного органа, сообщает личную информацию о собеседнике, тем самым вызывая доверие и психологически программируя на совершение определенных действий.

Таким образом, утечки конфиденциальных данных сегодня — это массовая, комплексная и важная проблема в мире и особенно в России. Она оказывает прямое влияние на важные аспекты жизнедеятельности социума: состояние делового климата, уровень доверия населения к цифровым продуктам, состояние киберпреступности, характер развития научного-технического прогресса, экономическое благополучие граждан. Цель данной статьи заключается в анализе трендов в области утечек конфиденциальных данных и социальных оснований данной проблемы.

Утечки конфиденциальных данных: тенденции, ключевые проблемы, социальные основания

Регулярные утечки конфиденциальных данных сегодня становятся нормой. По данным разработчика средств для информационной безопасности SearchInform, в первом полугодии 2020 г. данные в том или ином виде утекали из 91% российских компаний[10].

Неудивительно, что в этой связи рынок черных данных постоянно растет[11]. Сегодня этот рост обеспечивается далеко не только за счет профессиональных хакеров и взломщиков, но и благодаря действиям или бездействиям персонала организаций. Но каковы масштабы утечек по вине внутренних и внешних нарушителей? И какие цели они при этом преследуют? Каковы тренды в области утечек конфиденциальных данных в мире и в России? Специалисты группы компаний InfoWatch[12] в ежегодном отчете о количестве утечек данных ограниченного доступа предоставляют подробную информацию, в том числе относительно количества утечек (Рисунок 1).

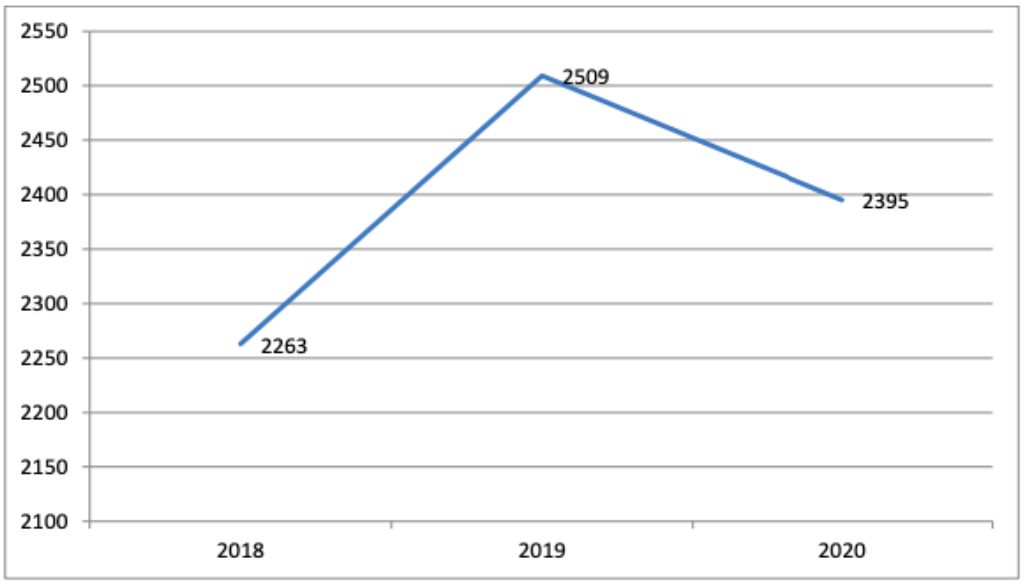

Рисунок 1. Число утечек информации, 2018–2020 гг.[13]

[10] «Большинство сотрудников не задумываются о том, что их мессенджеры контролируют»: как в России сливают конфиденциальную информацию и что за это бывает // Forbes [Электронный ресурс]. URL: https://www.forbes.ru/tehnologii/411175-bolshinstvo-sotrudnikov-ne-zadumyvayutsya-o-tom-chto-ih-messendzhery-kontroliruyut (дата обращения: 30.11.2021).

[11] Клиенты Сбербанка попали на черный рынок // Коммерсантъ [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4111863?from=main_1 (дата обращения: 24.10.2021).

[12] Группа компаний InfoWatch — российская компания, специализирующаяся на информационной безопасности в корпоративном секторе: защите корпораций от утечек информации и целевых атак извне.

[13] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).

Несмотря на снижение количества зафиксированных в 2020 г. инцидентов с утечками данных ограниченного доступа, составители отчета отмечают сохраняющуюся напряженность по данной проблеме. Спад, по мнению аналитиков, связан скорее не с фактическим снижением количества инцидентов, а с повышенным уровнем их латентности в период пандемии[14], а также со склонностью организаций скрывать от общественности факты инцидентов. Результаты исследования[15] компании SearchInform показывают, что в 2020 г. 57% опрошенных предпочитают полностью скрывать факты утечек данных[16]. Несмотря на положительную динамику (86% в 2017 г. и 63% в 2019 г.), процент желающих замолчать проблему остается достаточно высоким. Данная картинка кажется нам крайне показательной и в определенной степени отражает реальное отношение к проблемам информационной безопасности и безопасности данных клиентов в России и странах СНГ. Вместе с тем нельзя не отметить положительные тенденции в данном вопросе: с каждым годом компании все охотнее сами делятся фактами утечек из-за страха общественного порицания: есть риск столкнуться с более серьезной волной «народного гнева» и получить значительный удар по бренду[17].

Еще одна особенность утечек, которая занижает официальную статистику, заключается в том, что между фактом утечки и обнаружения этого инцидента может пройти значительный промежуток времени. Нередки случаи, когда система мониторинга информационной безопасности компании может быть настолько несовершенна, что проблемы обнаруживаются только после факта утечки данных [Иванова 2020, 102]. Как отмечают эксперты[18], массовый и быстрый переход сотрудников на удаленную работу в 2020 г. и неподготовленность системы информационной безопасности в некоторых организациях создали хорошие условия для компрометации конфиденциальных данных, и далеко не о всех фактах утечек во время локдауна известно общественности на текущий момент. Это подтверждает и статистика: наибольшая частота событий информационной безопасности случайного характера проявляется у новых сотрудников при модернизации рабочего окружения или при переходе на новую информационную систему [Беззатеев и др. 2021, 559].

Приведенные выше два тезиса говорят о том, что реальное количество произошедших в последние годы утечек значительно выше. Проблема в том, что не о всех из них известно на текущий момент или вообще станет известно общественности. Рассмотрим динамику распределения утечек по вектору воздействия (Рисунок 2).

[14] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[15] Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год. В исследовании приняло участие 1346 человек: начальники и сотрудники ИБ-подразделений, эксперты отрасли и руководители организаций из коммерческой, государственной и некоммерческой сфер.
[16] Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год // SearchInform [Электронный ресурс]. URL: https://searchinform.ru/uploads/sites/1/2021/03/issledovanie-urovnya-ib-v-rf-i-sng-za-2020-god.pdf (дата обращения: 30.11.2021).
[17] Приоткрытая информация: российские компании скрывают 57% утечек данных // Известия [Электронный ресурс]. URL: https://iz.ru/1121170/roman-kildiushkin/priotkrytaia-informatciia-rossiiskie-kompanii-skryvaiut-57-utechek-dannykh (дата обращения: 30.11.2021).
[18] Там же.

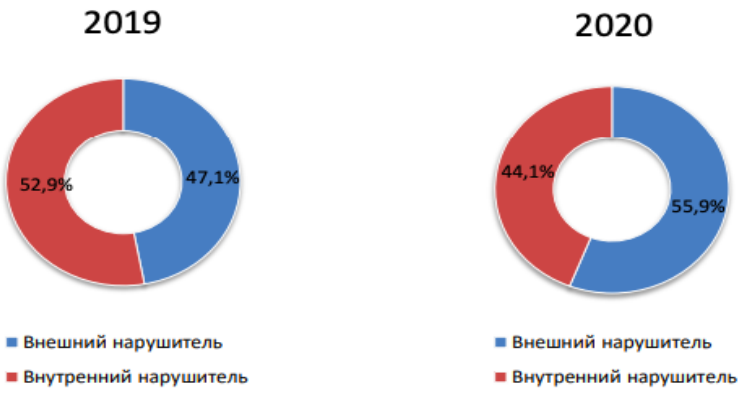

Рисунок 2. Распределение утечек по вектору воздействия, 2019–2020 гг.[19]

В 2020 г. отмечается существенный рост доли внешних нарушителей. Данные изменения динамики свидетельствуют о тех самых узких местах в системе информационной безопасности организаций, которые образовались вследствие стихийного перевода сотрудников на удаленную работу во время локдауна. В подтверждение данного тезиса свидетельствует факт нежелания или неготовности большой доли руководства организаций инвестировать средства, во-первых, в повышение информационной грамотности сотрудников, во-вторых, в защиту инфраструктуры организации.

Первый тезис ярко подтверждают результаты исследования[20], проведенного порталом Superjob[21]. Большинство опрошенных (68%) заявили о том, что никаких дополнительных требований по информационной безопасности и защите информации со стороны компании при переходе на удаленную работу выдвинуто не было. С нововведениями в политике информационной безопасности столкнулись только 16% респондентов, то есть примерно каждый 6 опрошенный. Среди внедренных новшеств участники опроса называли следующие: подписание дополнительного соглашения в сфере защиты информации (4%), обязательное использование VPN-каналов (2%), выдача корпоративного ноутбука со специальным ПО и установка компанией своего защитного ПО на личное устройство сотрудника (по 2%), использование защищенного соединения и двухфакторной аутентификации (по 1%), нахождение одному в комнате при работе с документами и копирование рабочих файлов на резервные устройства (по 1%). Еще 3% опрошенных отметили иные новшества: использование скрытых паролей, электронной подписи, неразглашение проблемы, использование только корпоративной почты и другие защитные методы. Данные «Лаборатории Касперского» показывают еще более тревожную картину: 79% россиян, перешедших на удаленную работу, не получали никаких конкретных рекомендаций по повышению цифровой грамотности и не прошли специальное обучение, призванное защитить сотрудников от киберрисков[22]. Данная неподготовленность сотрудников к удаленной работе как членов организаций наложилась

[19] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[20] В социологическом опросе приняли участие представители 1000 компаний и 1600 россиян с опытом работы в удаленном формате во время пандемии COVID-19. Исследование проходило 10–16 ноября 2021 года в 241 населенном пункте РФ.
[21] Большинство россиян не получало дополнительных требований по информационной безопасности при переходе на удаленку // Superjob [Электронный ресурс]. URL: https://www.superjob.ru/research/articles/113185/bolshinstvo-rossiyan-ne-poluchalo-dopolnitelnyh-trebovanij-po-informacionnoj-bezopasnosti-pri-perehode-na-udalenku/ (дата обращения: 30.11.2021).
[22] «Да кому мы нужны»: удаленка грозит бизнесу утечками и кибератаками // Известия [Электронный ресурс]. URL: https://iz.ru/1251988/ekaterina-korinenko/da-komu-my-nuzhny-udalenka-grozit-biznesu-utechkami-i-kiberatakami (дата обращения: 30.11.2021).

в целом на низкую цифровую грамотность россиян. Согласно мониторингу НАФИ[23], в 2021 г. только 27% населения обладает продвинутым уровнем цифровой компетенции. В условиях удаленной работы, когда уровень контроля снижается, а персонал чувствует себя более расслабленным, грань между рабочим и личным стирается, риск совершения ошибочных действий повышается, что ведет к росту утечек[24].

Ярким проявлением невысокого уровня цифровой грамотности россиян является сложившаяся культура обращения с собственными персональными данными. Согласно исследованию[25], проведенному Ipsos по заказу Visa, только 0.2% россиян знают, какую информацию по банковской карте и кому можно предоставлять, а также как отличить безопасный веб-сайт для оплаты в Интернете[26]. Поражают и другие выводы из исследования: 55% россиян согласны раскрыть личные данные в разговоре с мошенниками, а 65% не обращают внимание на адрес страницы при оплате в Интернете. При этом молодые люди в возрасте до 25 лет в меньшей степени осведомлены в вопросах защиты собственных персональных данных.

Ситуацию с неподготовленностью персонала и населения в целом по вопросам кибербезопасности усугубляет наличие факторов ограничения выделения средств на ИБ-бюджет. Об этом свидетельствуют результаты исследования[27] компании «Код безопасности»[28]: данную проблему отметили 39% опрошенных ИТ-специалистов в 2021 г. Для сравнения: в 2019 г. об этой проблеме упомянули 4% опрошенных, а в 2018 — только 2%. Выделим ключевые причины, которые приводят к ограничению бюджетов на информационную безопасность: тяжелое экономическое положение организаций во время пандемии; отсутствие понимания, зачем тратить средства на повышение информационной безопасности, или нежелание это делать. Эксперты отмечают пагубный подход, особенно распространенный в России, когда акцент делается не на профилактиках проблем в области информационной безопасности, а на авральном устранении уже случившихся инцидентов, «тушении пожаров»[29].

Распределение между внутренними и внешними нарушителями конфиденциальности данных представлено на Рисунке 3 и 4.

[23] Вынужденная цифровизация: исследование цифровой грамотности россиян в 2021 году // НАФИ [Электронный ресурс]. URL: https://nafi.ru/analytics/vynuzhdennaya-tsifrovizatsiya-issledovanie-tsifrovoy-gramotnosti-rossiyan-v-2021-godu/ (дата обращения: 30.11.2021).
[24] «Да кому мы нужны»: удаленка грозит бизнесу утечками и кибератаками // Известия [Электронный ресурс]. URL: https://iz.ru/1251988/ekaterina-korinenko/da-komu-my-nuzhny-udalenka-grozit-biznesu-utechkami-i-kiberatakami (дата обращения: 30.11.2021).
[25] Исследование проводилось в России для Visa компанией Ipsos. В опросе участвовали 1613 человек в возрасте от 18 до 65 лет: владельцы банковских карт и активные пользователи цифровых банковских услуг. Респонденты проживают в городах с населением от 100 тыс. человек.
[26] Visa оценила долю способных противостоять мошенникам россиян в 0,2%. С кем клиенты банков готовы делиться данными своих карт // РБК [Электронный ресурс]. URL: https://www.rbc.ru/finances/09/11/2021/6189163c9a794745fab97b07 (дата обращения: 30.11.2021).
[27] Исследование российского рынка информационной безопасности // Код безопасности [Электронный ресурс]. URL: https://www.securitycode.ru/documents/analytics/issledovanie-rossiyskogo-rynka-informatsionnoy-bezopasnosti-2021/ (дата обращения: 30.11.2021).
[28] Российский разработчик программных и аппаратных средств защиты информации.
[29] «Да кому мы нужны»: удаленка грозит бизнесу утечками и кибератаками // Известия [Электронный ресурс]. URL: https://iz.ru/1251988/ekaterina-korinenko/da-komu-my-nuzhny-udalenka-grozit-biznesu-utechkami-i-kiberatakami (дата обращения: 30.11.2021).

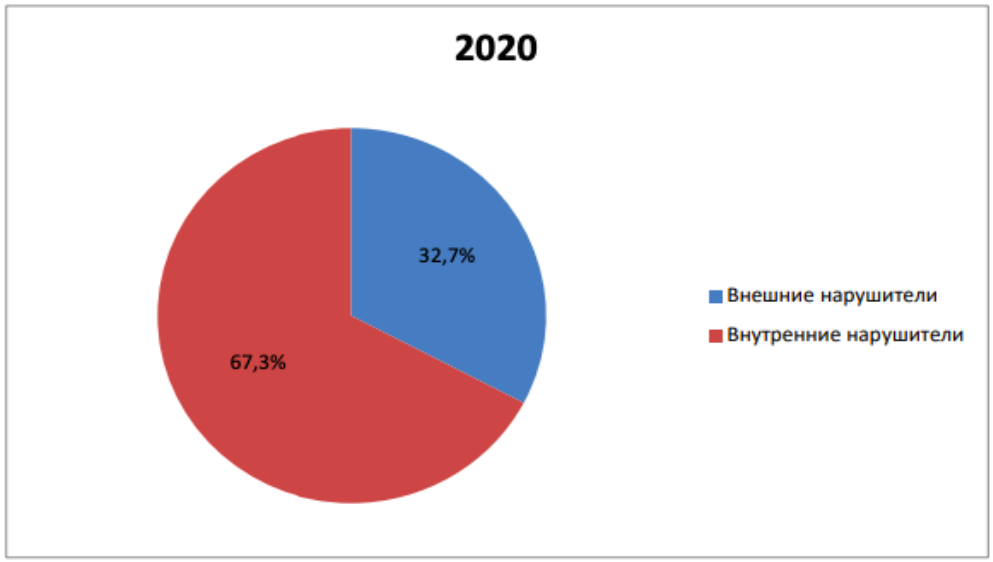

Рисунок 3. Доли общего объема записей, скомпрометированных в результате утечек по вине внешних и внутренних нарушителей, 2020 г. (%)[30]

В 2020 г. более двух третей от всего объема скомпрометированных данных приходилось на внутренних нарушителей — сотрудников организаций, в результате случайных и неслучайных действий или бездействий. Таким образом, именно персонал компании, а не внешние нарушители представляют главную угрозу с точки зрения объемов компрометируемых данных. С другой стороны, именно внешние нарушители опережали внутренних по количеству инцидентов с утечками в 2020 г., но при этом уступали в объемах скомпрометированных данных.

[30] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).

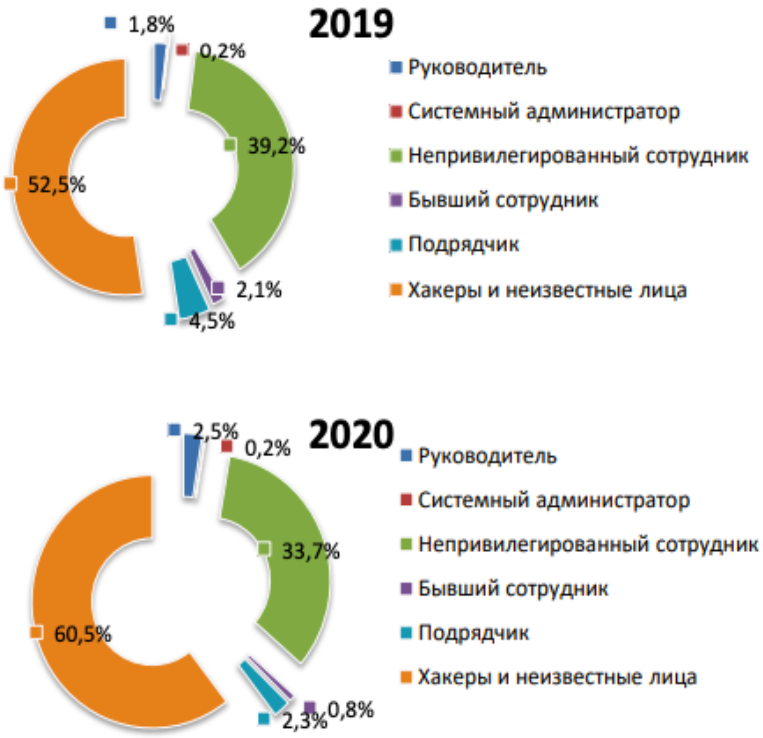

Рисунок 4. Распределение утечек по источнику (виновнику), 2019-2020 гг.[31]

Аналитики отмечают существенное снижение доли утечек по вине непривилегированных сотрудников, бывших сотрудников и подрядчиков организаций в 2020 г. по сравнению с прошлым годом. По всей видимости, руководство организаций извлекло урок из утечек данных, вызванных по вине рядовых сотрудников организаций, имеющих по роду деятельности доступ к конфиденциальным данным. Так, об ужесточении служебных правил и внедрении новых систем контроля при работе с данными заявило руководство «Сбербанка»[32] после инцидента с утечкой данных клиентов по вине сотрудника банка[33]. Нельзя не отметить новую угрозу, которая исходит от руководителей, имеющих более высокий уровень доступа: их доля среди всего объема нарушителей за год увеличилась с 1,8% до 2,5%.

Случай с утечкой данных в «Сбербанке» по вине сотрудника хорошо иллюстрирует тяжесть последствий утечек, вызванных внутренним нарушителем. Показательно распределение внутренних виновников инцидентов конфиденциальности: в России 41% — это менеджеры по работе с клиентами, 22% — бухгалтерия и финансисты, 20% — менеджеры снабжения[34]. Аналитики заключают, что наиболее уязвимыми становятся отделы, которые распоряжаются деньгами и критически важной корпоративной информацией. В такой ситуации серьезная утечка

[31] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[32] «Мы недооценили риски внутреннего предательства»: Сбербанк ужесточил правила работы с клиентскими данными // Forbes [Электронный ресурс]. URL: https://www.forbes.ru/newsroom/finansy-i-investicii/391587-my-nedoocenili-riski-vnutrennego-predatelstva-sberbank (дата обращения: 26.10.2021).
[33] Сбербанк завершил внутреннее расследование по выявлению канала утечки данных учетных записей по кредитным картам клиентов // Официальный сайт Сбербанка [Электронный ресурс]. URL: https://www.sberbank.ru/ru/press_center/all/article?newsID=56d223ed-1b37-48db-9790-1257c9c96d08&blockID=1303&regionID=77&lang=ru&type=NEWS (дата обращения: 26.10.2021).
[34] Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год // SearchInform [Электронный ресурс]. URL: https://searchinform.ru/uploads/sites/1/2021/03/issledovanie-urovnya-ib-v-rf-i-sng-za-2020-god.pdf (дата обращения: 30.11.2021).

может стоить для организации особенно дорого в плане клиентской базы или конкурентных преимуществ. В этой связи неудивительно, что среди опрошенных российских ИБ-специалистов 80% назвали внутренние инциденты более опасными, чем внешние[35].

Описанные выше тенденции в области киберугроз вынуждают проектировать инфраструктуры без периметра: система должна быть в высокой степени готова к атаке со стороны как внешнего, так и внутреннего нарушителя. Одна из наиболее популярных концепций в данной области — модель нулевого доверия. По данным Google Trends, интерес к данной концепции разработки и внедрения ПО постоянно растет во всем мире, особенно в последние несколько лет (Рисунок 5).

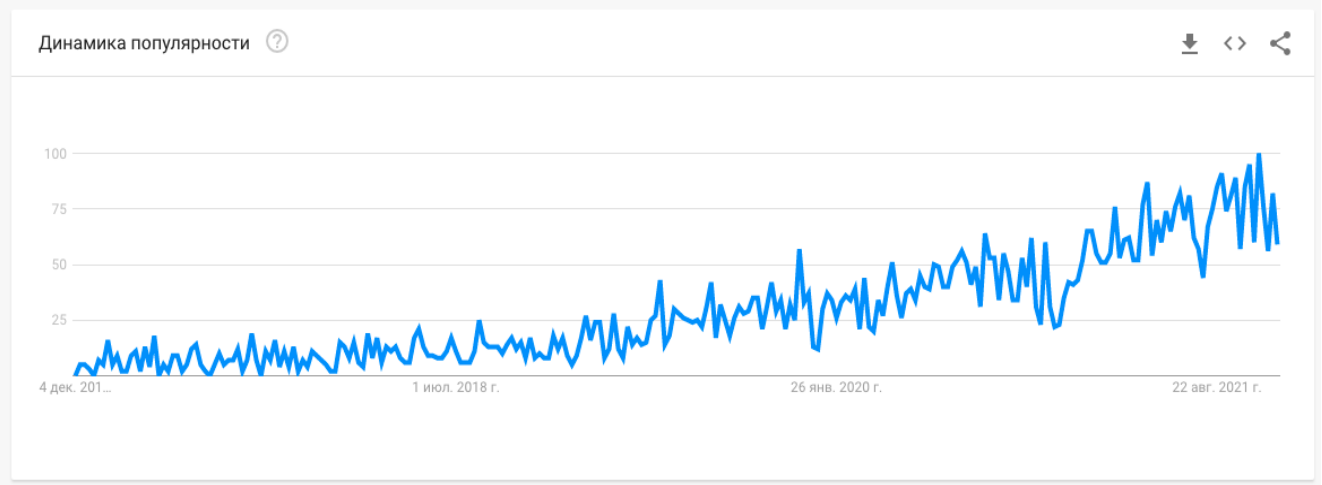

Рисунок 5. Динамика популярности запроса «Zero trust» в мире в 2016–2021 гг.[36]

Данный тренд подтверждают результаты исследования[37] компании Microsoft. Опрошенные лица, принимающие решения в области безопасности, назвали в 2021 г. приоритетом именно разработку стратегии нулевого доверия: 96% опрошенных отметили, что этот процесс является критичным для достижения целей организации. Подчеркивается, что смещение в сторону удаленного и гибридного формата занятости во время пандемии поспособствовали широкому распространению данной концепции: среди всех опрошенных респондентов, знакомых с моделью, 35% заявили о полном ее внедрении в своей организации, 42% находятся в процессе внедрения и еще 24% рассматривают возможность внедрения.

Модель нулевого доверия становится ответом организаций на рост масштаба и уровня последствий утечек по вине внутренних нарушителей. Концепт данной модели заключается в следующем: никогда не доверяй, всегда проверяй. Согласно подходу, каждый работник организации с точки зрения системы информационной безопасности воспринимается как потенциальная угроза. Верификация сотрудника требуется каждый раз, когда происходит попытка доступа к ресурсу или данным организации вне зависимости от должности или статуса данного сотрудника.

Какие тенденции в организационных процессах отражает широкое распространение концепции нулевого доверия в последние годы? С вынужденным массовым переходом на удаленный формат занятости человеческий фактор становится одной из главных причин

[35] Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год // SearchInform [Электронный ресурс]. URL: https://searchinform.ru/uploads/sites/1/2021/03/issledovanie-urovnya-ib-v-rf-i-sng-za-2020-god.pdf (дата обращения: 30.11.2021).
[36] Источник: Zero trust // Google Trends [Электронный ресурс]. URL: https://trends.google.ru/trends/explore?date=today%205-y&q=zero%20trust (дата обращения: 30.11.2021).
[37] Zero Trust Adoption Report // Microsoft Security [Электронный ресурс]. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha (дата обращения: 30.11.2021).

утечек конфиденциальных данных. В таких обстоятельствах концепция нулевого доверия представляет собой философское переосмысление управления безопасностью организации, которое требует изменения и организационной культуры[38], новые подходы к выстраиванию доверия к сотрудникам. С позиций нулевого доверия организация не воспринимается как единое образование, противопоставляющее себя враждебной окружающей действительности. Каждый сотрудник рассматривается как потенциальный нарушитель информационной безопасности организации, требуется постоянная верификация при доступе к конфиденциальным данным. Новые стандарты и модели взаимоотношений между сотрудниками и информационной системой — это ответ на новые вызовы для информационной безопасности организаций.

Теперь рассмотрим распределение утечек по типам данных (Рисунки 6 и 7).

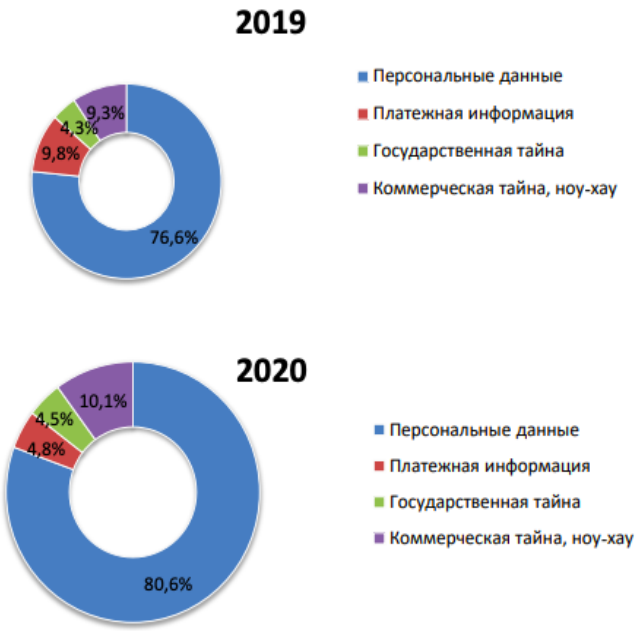

Рисунок 6. Распределение утечек по типам данных, 2019–2020 гг.[39]

Диаграмма наглядно иллюстрирует, что проблема утечки именно персональных данных сегодня особенно актуальна и массова. Обращает на себя внимание также более чем двойное снижение доли утечек платежной информации. По всей видимости, представители банковской отрасли сделали серьезные выводы из произошедших в последние годы резонансных случаев утечек данных клиентов и усилили системы безопасности при работе с конфиденциальными данными.

[38] Tech Trends 2021 // Deloitte [Электронный ресурс]. URL: https://www2.deloitte.com/content/dam/insights/articles/7024_TT-zero-trust-never-trust-always-verify/DI_2021-TT-zero-trust-never-trust-always-verify.pdf (дата обращения: 30.11.2021).
[39] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).

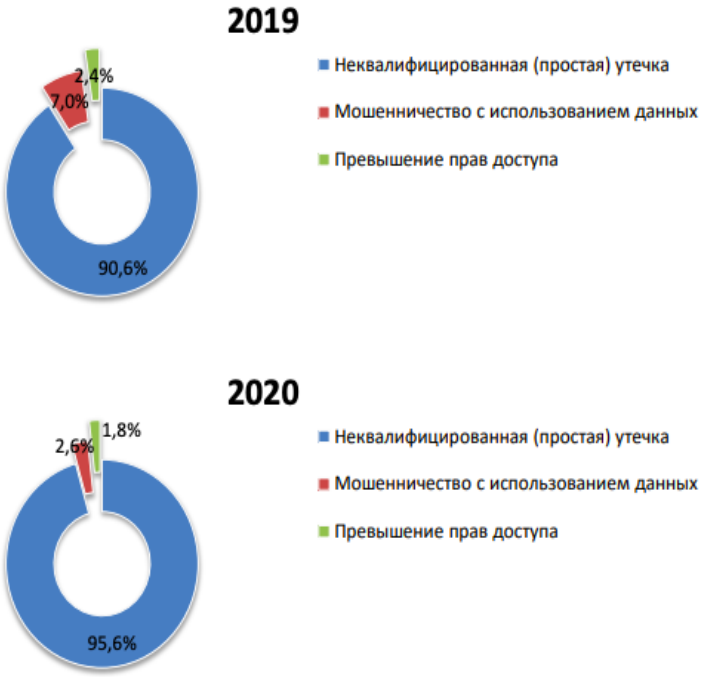

Рисунок 7. Распределение инцидентов по характеру, 2019–2020 гг.[40]

Обращает на себя внимание доля инцидентов, напрямую не связанных с мошенническими действиями. В 2020 г., как и в 2019, их доля составляла более 90%. То есть в подавляющем большинстве случаев нарушитель не использует скомпрометированные данные в мошеннических целях, а, как правило, старается как можно быстрее их продать[41]. Такое поведение можно объяснить разными причинами: страх серьезного наказания за мошеннические действия; непонимание, как иначе монетизировать украденные данные; боязнь разоблачения правоохранительными органами или службой безопасности организации. В таких условиях черный рынок персональных данных показывает стабильный рост[42]. Ситуация усугубляется тем, что злоумышленниками создаются все условия для простой и быстрой продажи скомпрометированных данных. Например, в мессенджере Telegram существуют специальные боты, которые позволяют анонимно зарабатывать на продаже данных[43]. Нередки случаи, когда украденная база, полностью исчерпав свой ресурс, выкладывается в открытый доступ и становится достоянием общественности[44].

Серьезный рост доли умышленных утечек отмечают эксперты в 2020 г. Если в 2019 г. только 60,2% утечек были совершены умышленно, то в 2020 г. показатель вырос до 72,5%[45]: то есть более двух третей инцидентов с утечками данных в 2020 г. совершались нарушителем сознательно. Эксперты отмечают, что такой существенный рост мог быть вызван несовершенством систем безопасности информационных систем организаций во время удаленной работы на фоне желания

[40] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[41] Там же.
[42] Побочное явление цифровизации: как в России крадут и продают персональные данные // Forbes [Электронный ресурс]. URL: https://www.forbes.ru/tehnologii/433651-pobochnoe-yavlenie-cifrovizacii-kak-v-rossii-kradut-i-prodayut-personalnye-dannye (дата обращения: 26.10.2021).
[43] Клерки поработали на хакеров // КоммерсантЪ [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4269795 (дата обращения: 30.11.2021).
[44] Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[45] Там же.

подзаработать со стороны недобросовестных сотрудников или взломщиков[46]. В целом в 2020 г. аналитики отмечают заметный рост утечек персональных данных по всем основным отраслям (Рисунок 8).

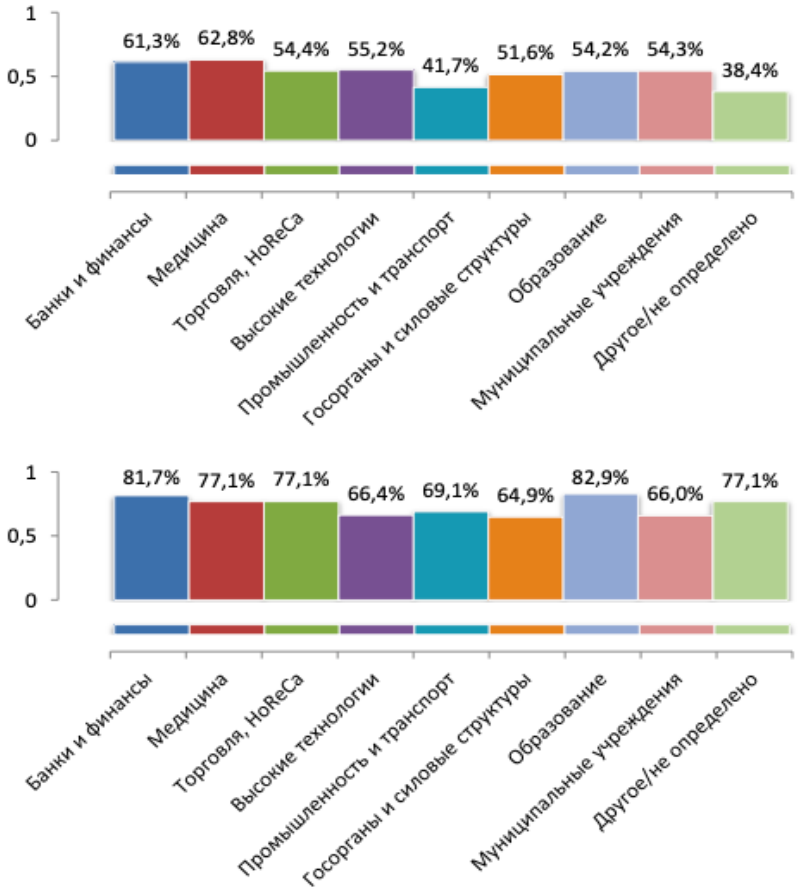

Рисунок 8. Доля умышленных утечек персональных данных от общего количества утечек персональных данных по отраслям, 2019–2020 гг.[47]

Отдельная большая группа инцидентов утечек данных связана с увольняющимися сотрудниками. Эксперты отмечают несколько причин, по которым работники совершают кражи[48] данных: это переманивание сотрудника к конкуренту, желание открыть собственный бизнес, месть нынешнему работодателю, манипуляции со стороны третьих лиц. Данные намерения подтверждает диаграмма распределения типов конфиденциальной информации, скомпрометированной увольняющимися нарушителями в 2020 г. (Рисунок 9).

[46] Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[47] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[48] Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).

Рисунок 9. Типы конфиденциальной информации, скомпрометированной увольняющимися нарушителями, 2020 г.[49]

Коммерческая тайна и передовые разработки организации — наиболее ценные данные, которые в большинстве случаев пытаются скомпрометировать увольняющиеся сотрудники. Возможности дальнейшего использования такой информации весьма амбициозны: от реализации в организации-конкуренте до запуска собственного бизнеса.

Защита конфиденциальных данных от неправомерного посягательства со стороны увольняющихся сотрудников — это неновая, но серьезная проблема для руководителей и службы безопасности организации. Анализ поведения пользователей на предмет умышленной и неумышленной возможности компрометации данных, отслеживание вероятности увольнения сотрудника, контроль уровня доступа к конфиденциальной информации и своевременная его блокировка при увольнении — важные аспекты информационной безопасности, которые требуют постоянного контроля и совершенствования. Компрометация данных именно со стороны увольняющихся сотрудников потенциально может привести к серьезным негативным последствиям для организации в виде оттока клиентов или потери положения на рынке, поскольку в половине случае корпоративная информация попадает к конкурентам[50].

Обсуждение результатов исследования

Новые вызовы цифровой эпохи требуют принципиально нового подхода к выстраиванию в том числе и социальных отношений, построения доверия к людям, организациям и институтам. Данный тезис был проиллюстрирован на примере концепции нулевого доверия, которая сейчас находится на волне популярности во всем мире. Теперь с точки зрения информационной безопасности организация не представляет собой гомогенную сущность, противопоставленную внешнему миру, а каждый ее член рассматривается как потенциальная угроза и нарушитель конфиденциальности. Это радикально новый подход, который полностью переворачивает традиционное представление о доверии: ни в коем случае не доверять, а постоянно проверять. Очевидно, в таких обстоятельствах организационная система в классическом ее понимании находится в состоянии противоречия: внедряется подход, который не соответствует самой сущности организации. Здесь необходимо подчеркнуть, что такая ситуация требует не только

[49] Источник: Исследование утечек информации ограниченного доступа в 2020 году // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения: 26.10.2021).
[50] Каждый второй случай кражи корпоративной информации сотрудником при увольнении из организации связан с передачей этих данных конкурентам // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/company/presscenter/news/20590 (дата обращения: 30.11.2021).

технологического, но и социального разрешения для снятия всех сложившихся противоречий. Но о каких социальных преобразованиях может идти речь? На наш взгляд, в условиях нулевого доверия такие организационные атрибуты, как, например, корпоративная культура, ценности, цели, стиль управления, могут потребовать серьезного пересмотра в новых обстоятельствах. Пресловутые слоганы об «одной команде», «большой семье» или «общих целях» в новых обстоятельствах серьезно расходятся с действительностью и требуют пересмотра в условиях, когда в каждом сотруднике видится нарушитель конфиденциальности.

В более глобальном смысле можно говорить о проблеме технологий в контексте устойчивого развития [Gidigbi 2021, 27]. В таких обстоятельствах вопрос обеспечения безопасности данных от внутренних нарушителей в организации — актуальный, но далеко не единственный аспект. Например, в последние годы набирает популярность использование в мошеннических целях технологий подделки голоса и изображения человека, фейковых аккаунтов и новостей. В этой связи авторитетные источники в лице The Guardian заявляют об угрозе демократии[51] — одному из столпов западного мира. И если с частью проблем эрудированный человек способен успешно справиться, то в случае других может разразиться настоящая «гонка вооружений»[52]. И такого рода вызовы требуют разрешения не только с точки зрения технологий, но и в первую очередь в социальной плоскости: пересмотр потребительского, близорукого отношения к технологиям; трансформация характера коммуникации между людьми в мессенджерах и социальных сетях; критическое мышлении в отношении информации из соцсетей и СМИ; трансформация доверия между людьми в соцсетях; регулирование лоббистской деятельности, особенно ИТ-гигантов[53]; пересмотр системы оценки руководителей компаний в сторону обеспечения высочайшего уровня защиты конфиденциальных данных [Helman 2019, 525]; внедрение новых подходов к обеспечению кибербезопасности, например кибериммунитета[54]; повышение влияния организаций по защите интересов пользователей; рост цифровой грамотности населения и изменение отношения к собственным персональным данным; пересмотр нормативно-правовой базы; создание условий гласности и общественного надзора. В противном случае без глубинной трансформации социального основания под обстоятельства нового технологического уклада фундаментальное решение проблемы кажется невозможным.

Заключение

Сейчас мы являемся свидетелями тех глобальных трансформационных процессов, которые меняют наше отношение к привычным, давно сложившимся вещам. И к этой трансформационной волне мы в высокой степени оказались не готовы. Процесс форсированной цифровизации, захлестнувший весь мир в последние годы, ярко показал несовершенства самого разнообразного порядка: коллективную и индивидуальную безответственность к защите данных и информационной безопасности, изъяны нормативно-правовой базы, нежелание и неготовность инвестировать ресурсы в повышение уровня цифровой грамотности и защиту инфраструктуры от киберугроз, кризис доверия в организациях. Более глобально — отсутствие единого, последовательного, сбалансированного, системного подхода к цифровой трансформации; глубокого понимания ее основ и первопричин, как технических, так и социальных; тщательной

[51] The rise of the deepfake and the threat to democracy // The Guardian [Электронный ресурс]. URL: https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy (дата обращения: 02.12.2021).
[52] Как защититься от дипфейков // Kaspersky Daily [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/rsa2020-deepfakes-mitigation/27678/ (дата обращения: 02.12.2021).
[53] Amazon wages secret war on Americans' privacy, documents show // Reuters [Электронный ресурс]. URL: https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/ (дата обращения: 15.12.2021).
[54] Почему традиционный подход к кибербезопасности устарел — Kaspersky // РБК Pro [Электронный ресурс]. URL: https://pro.rbc.ru/news/610b597e9a79471077e87133?from=material_cards (дата обращения: 15.12.2021).

проработки возможных последствий; моделирования рисков и потенциальных угроз; четкого и методичного плана по осуществлению цифровой трансформации. Данное непонимание выливается сегодня в распространенное «тушение пожаров» и «латание дыр» уже по факту свершения инцидентов, причем данная практика имеет место среди как небольших организаций, так и международных корпораций и целых государств. Это слабые, реактивные, бессистемные ответы на глобальную, зачастую неконтролируемую в нынешних условиях цифровую волну. В таких обстоятельствах запрос на сбалансированное цифровое развитие становится все более актуальным, и в этом заинтересованы все стороны: государство, бизнес, население. Важно осознать, что технологии сегодня, их внедрение и использование — это не решение всех проблем в короткий срок, а огромная, сложная и кропотливая работа с большими рисками и потенциальными выигрышами. Использование технологий по модели черного ящика без глубинного понимания их возможностей и опасностей имеет губительную перспективу, и события последних лет это ярко показывают. Запрос на устойчивое цифровое развитие должен проявляться все отчетливее. По всей видимости, в ближайшие годы вопрос об устойчивом цифровом развитии, выработке и реализации грамотного, системного, рационального подхода к технологическим трансформациям должен стать одним из главных в мировой повестке.

Список литературы:

Беззатеев С.В., Елина Т.Н., Мыльников В.А., Лившиц И.И. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 4. С. 553–561. DOI: 10.17586/2226-1494-2021-21-4-553-561

Иванова А.П. Утечка персональных данных: большая проблема в цифровую эпоху (обзор) // Реферативный журнал Государство и право. 2020. № 4. С. 100–107.

Перекрестова В.А., Фурсова П.В. Цифровизация в России: проблемы информационной безопасности // Вестник Прикамского социального института. 2021. № 2 (89). С. 170–176.

Сергеева И.Г., Али Х.М. Анализ технологических рисков финансовых инноваций // Научный журнал НИУ ИТМО. 2021. № 2. С. 23–29. DOI: 10.17586/2310-1172-2021-14-2-23-29

Bayan A., Beloff N., White M. Rise of Big Data — Issues and Challenges // 21st Saudi Computer Society National Computer Conference (NCC). 2018. DOI: 10.1109/NCG.2018.8593166

Gidigbi M.O. Digital Technologies for Sustainable Development: Dual Challenge of Sustainability and Inclusivity Perspective // Law & Digital Technologies. 2021. Vol. 1. P. 27–36. DOI: 10.18254/S123456780015729-2

Hammouchi H., Cherqi O., Mezzour G., Ghogho M., Koutbi M. Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches over Time // Procedia Computer Science. 2019. Vol. 151. P. 1004–1009. DOI: https://doi.org/10.1016/j.procs.2019.04.141

Helman L. Pay for (Privacy) Performance Holding Social Network Executives Accountable for Breaches in Data Privacy Protection // Brooklyn Law Review. 2019. Vol. 84. № 2. P. 523–569.

Marcus D.J. The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information // Duke Law Journal. 2018. Vol. 68. № 3. P. 555–593.

Stier S., Breuer J., Siegers P., Thorson K. Integrating Survey Data and Digital Trace Data: Key Issues in Developing an Emerging Field // Social Science Computer Review. 2020. Vol. 38. Is. 5. P. 503–516. DOI: https://doi.org/10.1177/0894439319843669

References:

Bayan A., Beloff N., White M. (2018) Rise of Big Data – Issues and Challenges. *21st Saudi Computer Society National Computer Conference (NCC)*. DOI: 10.1109/NCG.2018.8593166

Bezzateev S.V., Elina T.N., Mylnikov V.A., Livshitz I.I. (2021) Risk Assessment Methodology for Information Systems, Based on the User Behavior and IT-Security Incidents Analysis. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki.* Vol. 21. № 4. P. 553–561. DOI: 10.17586/2226-1494-2021-21-4-553-561

Gidigbi M.O. (2021) Digital Technologies for Sustainable Development: Dual Challenge of Sustainability and Inclusivity Perspective. *Law & Digital Technologies*. Vol. 1. P. 27–36. DOI: 10.18254/S123456780015729-2

Hammouchi H., Cherqi O., Mezzour G., Ghogho M., Koutbi M. (2019) Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches over Time. *Procedia Computer Science*. Vol. 151. P. 1004–1009. DOI: https://doi.org/10.1016/j.procs.2019.04.141

Helman L. (2019) Pay for (Privacy) Performance Holding Social Network Executives Accountable for Breaches in Data Privacy Protection. *Brooklyn Law Review*. Vol. 84. № 2. P. 523–569.

Ivanova A.P. (2020) Utechka personal'nykh dannykh: bol'shaya problema v tsifrovuyu epokhu (obzor) [Personal data leak: The big problem in the digital age (overview)]. *Referativnyy zhurnal Gosudarstvo i pravo*. № 4. P. 100–107.

Marcus D.J. (2018) The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke Law Journal.* Vol. 68. № 3. P. 555–593.

Perekrestova V.A., Fursova P.V. (2021) Digitalization in Russia: Problems of Information Security. *Vestnik Prikamskogo sotsial'nogo instituta*. № 2 (89). P. 170–176.

Sergeeva I.G., Ali H.M. (2021) Technological Risk Analysis of Financial Innovations. *Nauchnyy zhurnal NIU ITMO*. № 2. P. 23–29. DOI: 10.17586/2310-1172-2021-14-2-23-29

Stier S., Breuer J., Siegers P., Thorson K. (2020) Integrating Survey Data and Digital Trace Data: Key Issues in Developing an Emerging Field. *Social Science Computer Review*. Vol. 38. Is. 5. P. 503–516. DOI: https://doi.org/10.1177/0894439319843669

Дата поступления/Received: 26.12.2021