ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.37468/2307-1400-2022-3-52-75

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРИ УТЕЧКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

***Гайсина Алина Ринатовна*[1]**
***Зайцев Александр Константинович*[1]**
***Матвеев Владимир Владимирович*[1]**

[1]Санкт-Петербургский государственный экономический университет, Санкт-Петербург, Россия

АННОТАЦИЯ

Выявлена актуальность противодействия утечки конфиденциальной информации в связи с активной цифровизацией процессов управления, цифровой экономики, расширением масштабов удаленной работы. Указано появление и расширение нового вида ренты – конфиденциальной информации. Установлены тенденции в сфере утечки конфиденциальной информации. Дано понятие утечки информации и смоделированы схемы утечки. Проанализировано изменение структуры воздействия на информационные ресурсы. Систематизированы факторы умышленных утечек конфиденциальной информации. Проведена классификация потерь от утечек конфиденциальной информации. Описан форум Dark web по продаже конфиденциальной информации. Проанализированы отрасли и подразделения утечки конфиденциальной информации. Проведен хронологический анализ государственных структур, подверженных утечке конфиденциальной информации. Представлен международный опыт по противодействию утечки конфиденциальной информации. Проведен сравнительный анализ утечки конфиденциальной информации в России и в странах мира по отраслям, размеру организаций, по характеру информации.

Ключевые слова: утечки, рентная экономика, экономическая безопасность, информационная безопасность, гибридные атаки, внешние нарушители, внутренние нарушители, хаккеры, Dark web, DLP-системы, аутоведомственная платформа, криминализация, InfoWatch, латентность, финансовые потери, стоимость утечки данных.

ENSURING ECONOMIC SECURITY IN CASE OF LEAKAGE OF CONFIDENTIAL INFORMATION

***Gaysina A. R.*[1]**
***Zaitsev A. K.*[1]**
***Matveev V. V.*[1]**

[1]St. Petersburg State University of Economics, St. Petersburg, Russia

ABSTRACT

The relevance of countering the leakage of confidential information in connection with the active digitalization of management processes, the digital economy, and the expansion of remote work has been identified. The emergence and expansion of a new type of rent - confidential information is indicated. Tendencies in the field of leakage of confidential information have been established. The concept of information leakage is given and leakage schemes are modeled. The change in the structure of the impact on information resources is analyzed. The factors of intentional leaks of confidential information are systematized. The classification of losses from leaks of confidential information is carried out. The Dark web forum for selling confidential information is described. The branches and divisions of confidential information leakage are analyzed. A chronological analysis of state structures exposed to the leakage of confidential information was carried out. The international experience in countering the leakage of confidential information is presented. A comparative analysis of the leakage of confidential information in Russia and in the countries of the world by industry, size of organizations, and the nature of information has been carried out.

Keywords: leaks, rental economy, economic security, information security, hybrid attacks, external intruders, insiders, hackers, Dark web, DLP systems, auto-departmental platform, criminalization, InfoWatch, latency, financial losses, cost of data leakage.

Введение

Обеспечение экономической безопасности, как свойство функционирования управляемой системы с предсказуемым достижением целевой функции в пределах допустимых отклонений под воздействием внешних факторов среды, внутренних изменений системы и управления ориентировано за защиту от внешних и внутренних угроз для устойчивого по предсказуемости функционирования управляемой системы [1].

Внедрение современных информационно-коммуникационных технологий, с одной стороны, обеспечивает рост быстродействия экономических процессов, расширяет технологические возможности производства и обмена, а, с другой стороны, увеличивает уязвимость управляемых систем к угрозам потери информации в силу растущей зависимости от информационно-коммуникационных средств и действий персонала [2].

Особенным явился период пандемии, возникшей по причине COVID-19, когда принципиально изменился процесс экономической деятельности, связанный с необходимостью перехода многих субъектов экономики на удаленную работу. В связи с этим возросли риски утечки конфиденциальной информации [3]. Так, по экспертной оценке, за первое полугодие 2020 года потери российского бизнеса от утечек информации составили около 1,800 трлн. рублей. За второе полугодие этот показатель снизился и составил около 1,2 трлн. рублей. Снижение потерь связано с тем, что, приобретя некоторый опыт удаленной работы и оценив экономические потери, субъекты экономики начали активно работать над проблемой обеспечения информационной безопасности (ИБ) [4].

В рентной экономике, которую еще называют капитализмом, основой сохранения и преумножения капитала является рента, которой могут быть: земля, право эмиссии средств платежа, ссудный процент, природные богатства и т.д. [5]. В настоящее время одной из форм товарной ренты стала конфиденциальная информация.

Товарная рента – та прибыль, которая зарабатывается при производстве товаров или преобразовании информации. Её извлечение является процессом фундаментальным для расширенного воспроизводства капитала, лежащим в основании всех остальных экономических процессов.

Формально ферментом, катализирующим и оживляющим товарные циклы, является прибыль, а фактически – жажда наживы. Именно она заставляет крутить товарные циклы, обеспечивая расширенное воспроизводство (рис. 1). Функцию эквивалента ресурсов прибыли свободного капитала исполняли пользовавшиеся устойчивым спросом товары длительного хранения. Мир наполнен массой товаров, в которой возникают новые товары и в настоящее время, в частно-

Рисунок 1 – Цикл обмена в рентной экономике

сти, появился новый товар – конфиденциальная информация. В связи с этим появился новый фактор угроз национальной и экономической безопасности – утечка конфиденциальной информации.

Тенденции в сфере утечки конфиденциальной информации

По данным исследований, проведенных экспертно-аналитическим центром InfoWatch за 2021 г. зарегистрирована 331 утечка конфиденциальной информации из коммерческих компаний, органов власти и государственных организаций в России [6]. Это на 40,8% меньше, чем в 2020 г., и на 46,4% меньше, чем в аномальном 2019 г. (рис. 2).

Снижение числа зарегистрированных утечек можно объяснить ослаблением контроля за сотрудниками в период удаленной работы, в этой ситуации многие инциденты могли оказаться в тени. К тому же возникли новые возможности для злоумышленников. Но вместе с тем, ряд крупных компаний и госорганизаций начали получать эффект от внедренных в предыдущие годы средств защиты информации, в том числе DLP-систем, получая информацию об ошибках персонала, о попытках (в том числе удачных) копирования защищаемых данных [7]. И как следствие, успешное предотвращение утечкам конфиденциальной информации [8].

В то же самое время одними из причин сохранения значительной степени утечки конфиденциальной информации являются:

– расширение и распространение технологий, которые обеспечивают более широкий несанкционированный доступ к информации организаций, чем это было прежде (облачные провайдеры). Третьи лица могут получать информацию через цепочку поставок, клиентов и поставщиков.
– увеличение числа устройств, которые используются для обмена данными.

Традиционные программные и организационные средства обеспечения информационной безопасности постепенно устаревают, что вызывает необходимость в новых средствах анализа угроз и программах безопасности для снижения рисков и выявления информационных атак.

Анализируя содержание информации, ставшей достоянием злоумышленников, следует отметить, что основную утекшую конфиденциальную информацию составляют персональные данные и платежная информация. В 2021 г. в открытых источниках появилась информация об утечке более 80 млн записей персональных данных и платежной информации, что примерно на 20% больше, чем в 2020 г. (рис. 3). Однако следует отметить, что на теневом онлайн-рынке Dark web в 2021 г. активно распространялись базы данных и их фрагменты из утечек прошлых лет [9].

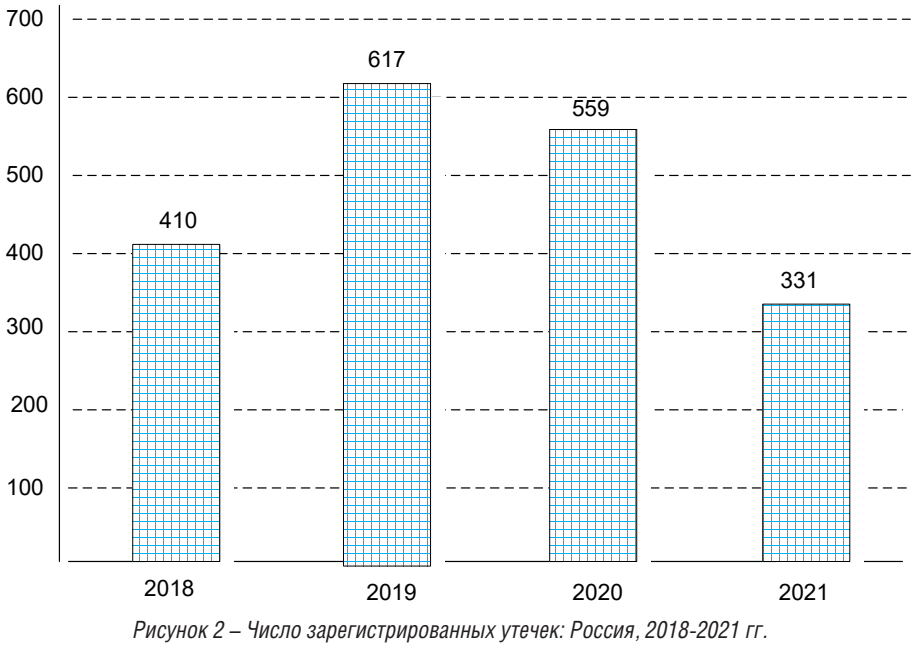


Рисунок 2 – Число зарегистрированных утечек: Россия, 2018-2021 гг.

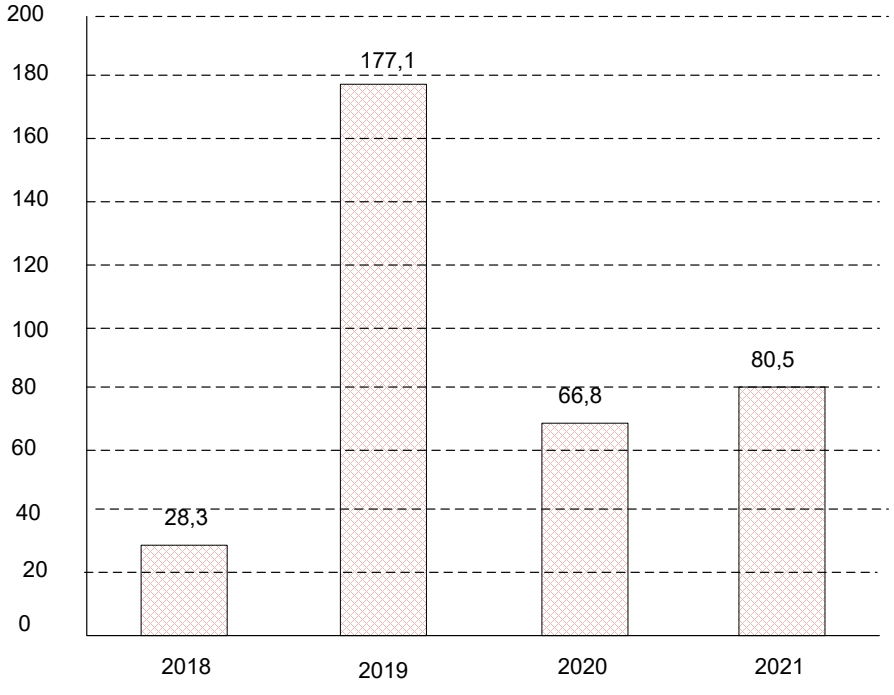


Рисунок 3 – Количество утекших записей: Россия, 2018-2021 гг.

Можно сделать промежуточный вывод о том, что в 2021 году в России наметилась тенденция роста количества утечек персональных данных и платёжной информации.

Понятие утечки информации и схемы утечки

Утечка информации – это кража данных, которая является серьезной проблемой для экономической безопасности хозяйствующего субъекта. В этих условиях особую актуальность приобретают вопросы обеспечения экономической безопасности с точки зрения защиты конфиденциальной информации [10].

Источниками утечки конфиденциальной информации могут как внешние, так и внутренние нарушители.

Схема действий внешних нарушителей представлена на рис. 4.

При краже данных внешними нарушителями используется одна из двух схем.

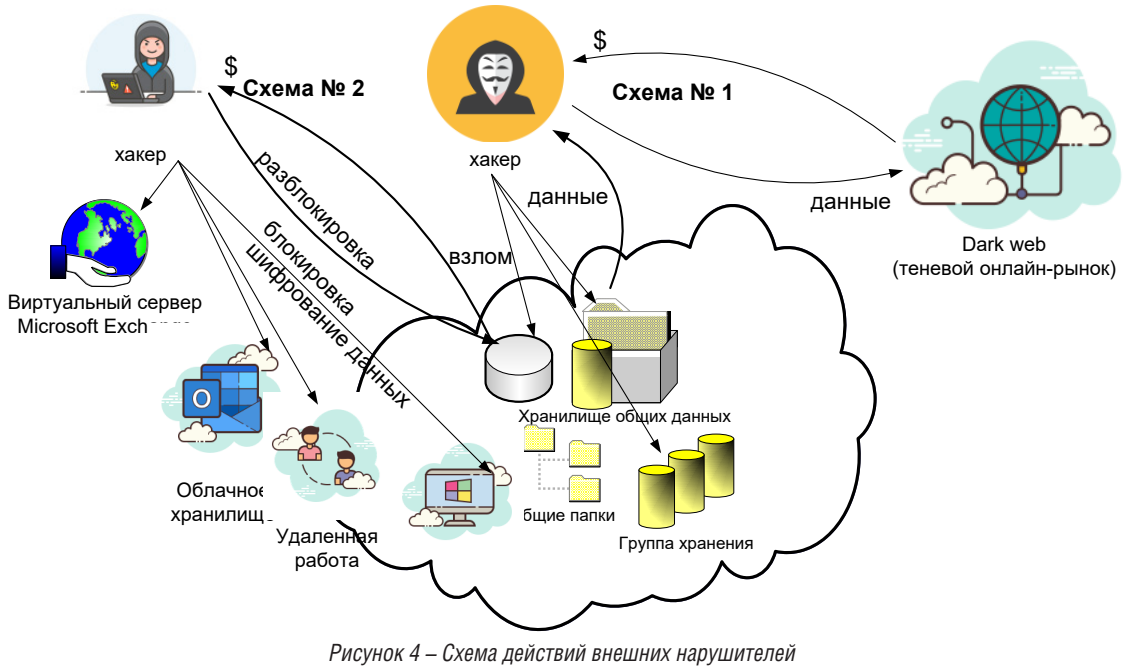


Рисунок 4 – Схема действий внешних нарушителей

Схема №1: «взлом – копирование данных – продажа данных – деньги».

Схема №2 с использованием шифрования данных пользователя. Это выглядит так: «взлом – шифрование данных – деньги». Данная схема исключает длительный и неопределенный по времени этап продажи, например, в Dark web, если только это не была заказная акция.

Остановка бизнес-процессов в результате шифрования данных и последующей блокировки информационных систем, цифровых сервисов – это крайне болезненная ситуация для большинства компаний. Причем не всегда помогает наличие резервных копий, так как необходимо время на восстановление и тестирование. Поэтому в подобной ситуации бизнес зачастую идёт на диалог с киберпреступниками и вносит требуемый выкуп.

То есть «конверсию» атак хакеры чаще стали рассматривать под другим углом – «прямой монетизации» данных в деньги (выкуп за расшифровку), исключив процесс поиска покупателей данных и непосредственной продажи, снизив тем самым количество объявлений в Dark web и, как следствие, повлияв на снижение публикаций об утечках в СМИ [11].

Структура воздействия на информационные ресурсы

За 2021 г. произошли изменения в структуре утечек с точки зрения вектора воздействия на информационные ресурсы (внешний/внутренний). Доля утечек по вине внешних нарушителей в 2021 г. по сравнению с 2020 годом выросла с 52,9% до 63,2%. Соответственно, в результате умышленных и случайных действий внутренних нарушителей произошло снижение утечек до 36,8% из общего количества в 2021 г. по сравнению с 47,1% в 2020 г. (рис. 5).

Вероятно, сыграло свою роль распространение удаленной работы, когда контроль за сотрудниками оказался сильно затруднен. В такой ситуации недобросовестные работники могли незаметно похищать информацию, кроме того, в тень мог уйти большое количество случайных нарушений.

В целом, с 2018 г. наблюдается неуклонный рост доли утечек в результате действий внешних нарушителей. Это может быть связано со становлением широкого спектра хакерских группировок, повышением доступности вредоносного ПО (в том числе по мере развитие модели RaaS – «вредоносное ПО как услуга»). Вместе с тем, в ряде случаев возможно предположить, что утечки были совершены при участии сотрудников, вступивших в сговор с хакерами, или вследствие ошибок сотрудников, которые привели к раскрытию аутентификационной информации, которой воспользовались внешние нарушители. Но в других случаях, когда утечку удалось предотвратить или своевременно выявить, минимизировав ущерб, многие компании убедились в эффективности средств защиты, направленных на проти-

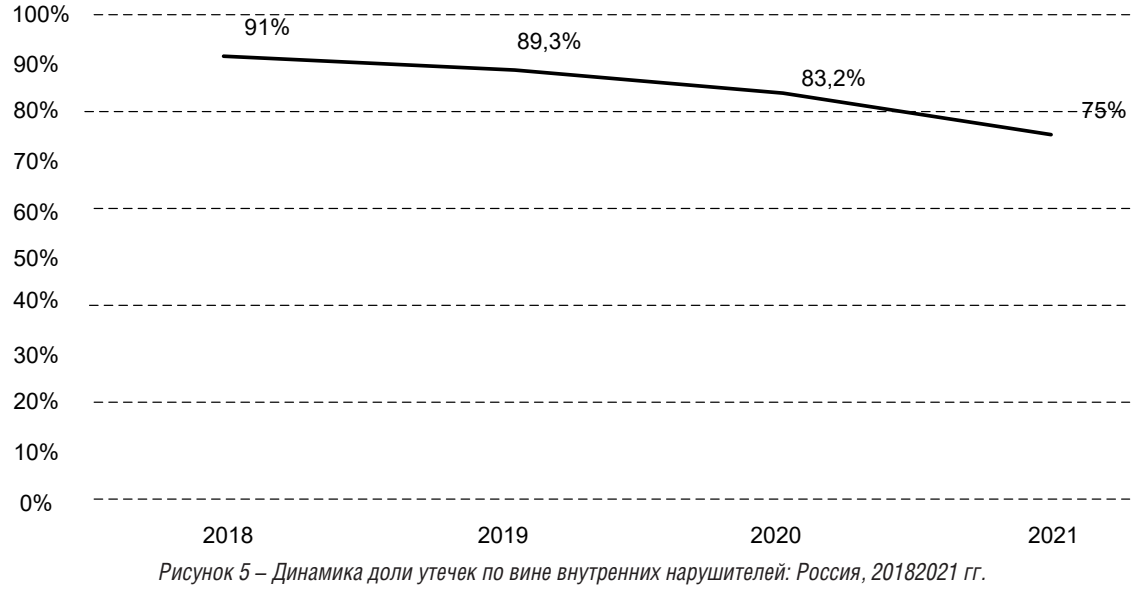


Рисунок 5 – Динамика доли утечек по вине внутренних нарушителей: Россия, 20182021 гг.

водействие внутренним нарушениям. Речь идет о DLP-системах, решениях для контроля доступа, поведенческой аналитики и т.д. [12].

Умышленные утечки конфиденциальной информации

Статистика указывает на то, что в период пандемии резко выросла доля утечек умышленного характера: с 58% в 2019 г. до 83% в 2020-2021 гг. (рис. 6).

Причиной этому послужило несколько факторов [13]:

- в значительной степени возросла хакерская активность при общем ослаблении контроля за персоналом в условиях удаленной работы;
- возросла цена на черном рынке персональных данных и другой конфиденциальной информации;
- в период пандемии возрос объем данных и/или появились новые обширные источники персональных данных, что связано с созданием новых баз данных: заболевших, вакцинированных, получивших социальную поддержку и т.д.;
- в значительной степени возросли в объемах некоторые сервисы, например, служб по доставке еды.

Все это способствовало росту охотников за конфиденциальной информацией как внутри организаций, так и за ее пределами [14].

Продажа данных в Dark web

Dark web или по-другому «Darknet», что означает темный интернет, а также употребляется понятие «Deep Web» – глубокая паутина, представляет собой часть теневого онлайн-рынка. Dark web – это специализированная группа сайтов, где личность каждого пользователя скрыта от власти, трекеров и правоохранительных органов. Стандартные поисковые системы и стандартные веб-браузеры не видят страницы Dark web. То есть это частное виртуальное пространство, где люди действуют анонимно для достижения своих целей [15].

Основное свойство Dark web – полная анонимность онлайн с гарантией безопасности, где пользователи могут виртуально взаимодействовать друг с другом и не бояться закона. Dark web содержит форумы, блоги информаторов, услуги сводничества одних с другими, онлайн рынки, ресурсы с документацией и т.д.

На Dark web информаторы сообщают о корпоративных и правительственных неправомерных действиях прессе без опасений преследования, рассекречивают коррупционные действия, которые скрыты от общественности, свободно излагают информацию вне зависимости от политических, религиозных и расовых убеждений, не опасаясь репрессий [16].

Но Dark web – это и черный рынок, где можно

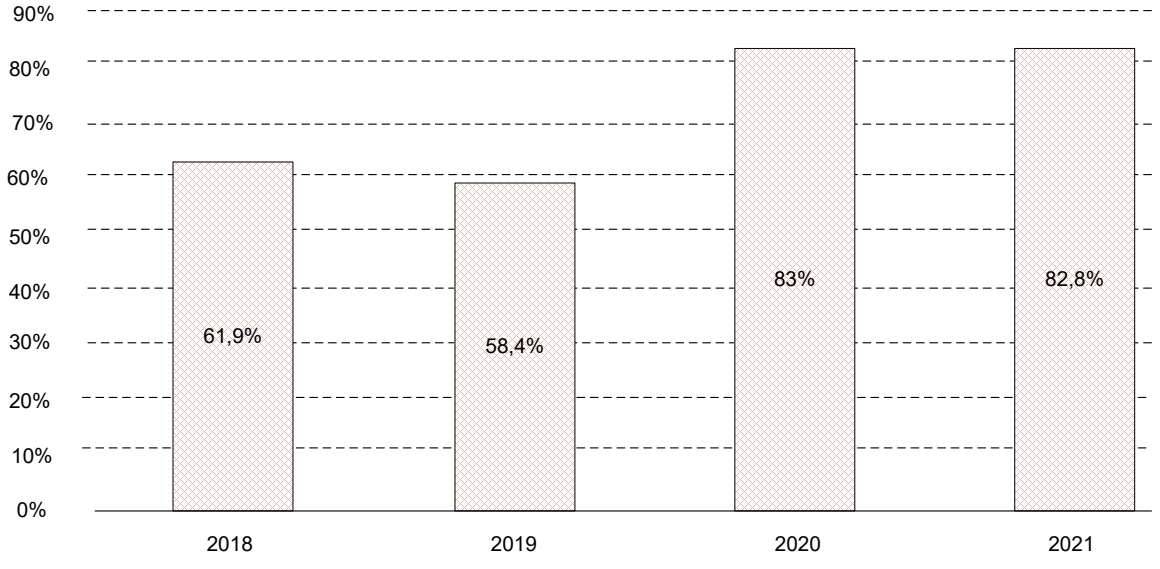


Рисунок 6 – Динамика доли умышленных утечек: Россия, 2018-2021 гг.

купить или продать что угодно, любую контрабанду, украденную вещь или незаконно добытую информацию. Наркотики, оружие, ворованные номера кредитных карт, порнографию, услуги по отмыванию денег и даже наем убийц. В том числе можно купить и продать любую конфиденциальную информацию.

Работы в Dark web требует установки и использования специального программного обеспечения, и высокий профессионализм в IT-технологиях. Работу анонимной обеспечивают две разные технологии: протокол I2P (Invisible Internet Project) и протокол TOR (The Onion Router).

TOR представляет из себя систему прокси-серверов, позволяющих устанавливать анонимное сетевое соединение, защищённое от прослушивания. Сайты TOR используют имя домена .onion [17].

Сеть I2P является оверлейной, устойчивой (отключение узла не повлияет на функционирование сети) и анонимной. При передаче данных между узлами сети применяется шифрование. В скорости работы уступает TOR, но зато I2P более устойчива перед правоохранительным надзором. В обоих случаях Dark web работает с использованием сложного математического шифрования, чтобы зашифровать личность, сеть и местонахождение участника. Весь сетевой трафик перескакивает с сервера на сервер по всему миру, что делает отслеживание невозможным. Обмен сообщениями осуществляется с помощью псевдонимов, не связанных с настоящей личностью. Большинство денежных операций используют биткойны и услуги депонирования в третьем лице, чтобы защитить покупателя и продавца от нечестной торговли.

Оплата товаров и услуг в Dark Web осуществляются с использованием анонимных номеров счетов (также, как счета в швейцарских банках, но с большей маскировкой). Эти анонимные счета называются «биткойн кошелек». Биткойн является не регулируемой валютой, поэтому в случае обмана или нечестной финансовой операций не получится обратиться в банк для возврата денег.

В Dark Web предпочитаются биткойны. Услуга депонирования в третьем лице будет действовать как от имени покупателя, так и от имени продавца, действуя в качестве доверенного посредника в обмен на комиссионные.

Контрабандные товары Dark Web доставляются обычной почтой или курьерской службой. Степень риска покупки на Dark Web зависит от действий правоохранительных органов. Доставка конфиденциальной информации и оплата за нее биткоинами фактически исключает вмешательство правоохранительных органов.

Классификация потерь от утечек конфиденциальной информации

Утечки конфиденциальной информации приводят к:

– репутационным потерям;
– финансовым потерям.

Финансовые потери от утечек конфиденциальной информации в организации

Их последствия могут быть серьезными. Так, согласно подсчетам экспертов, достаточно утраты всего 20% коммерческих секретов субъекта хозяйствования, чтобы спровоцировать его банкротство.

Подобные примеры есть в мировой практике. Например, в 2019 году крупный американский медицинский коллектор Retrieval-Masters Creditors Bureau Inc, один из лидеров отрасли, обанкротился как раз из-за того, что было допущено утекание сведений о более чем 12.000.000 клиентов. Компания не смогла справиться с обязательствами по выплате $4.000.000 компенсаций потерпевшим, в результате чего было принято решение инициировать процедуру признания агентства банкротом.

Даже потери от утечек 5% конфиденциальных данных компании приводят к серьезным последствиям. Эксперты отмечают, что такого количества достаточно для утраты лидирующих позиций на рынке.

К финансовым потерям относятся прямой денежный, а также вероятный ущерб, возникающий из-за того, что компания лишается части прибыли.

Утечки важных данных в организации приводят к возникновению (а если не принять меры, то к реализации) нескольких видов финансовых рисков:

Liquidity risk. Риск ликвидности, заключается в неспособности компанией выполнять свои финансовые обязательства (перед заемщиками, поставщиками и пр.). Подобные риски возникают из-за утечек информации, вследствие которых снижается эффективность работы компании: из-за корпоративного мошенничества, хищения материальных активов, сырья.

Market risk. Рыночный риск, заключается в снижении стоимости активов. Практика показывает, что подобные инциденты влекут потерю стоимости акций крупных организаций на срок около 3 месяцев. У кого-то после этого у многих происходит рост до прежних показателей, другим же компаниям достичь первоначального уровня не удается.

Operation risk. Операционные риски связаны непосредственно с выполнением компанией бизнес-функций. Довольно опасны для организации, так как при их возникновении потери от утечек информации имеют непредвиденный характер.

Последствия реализации всех трех групп рисков проявляются для компаний по-разному. Кому-то приходится возмещать немалый ущерб сотрудникам или клиентам (как в примере с Retrieval-Masters Creditors Bureau Inc). Кто-то теряет прибыль на том, что украденные технологии попадают в руки конкурентов, а те отбирают часть рынка. У каких-то бизнес-субъектов падает стоимость активов, акций.

Репутационные потери от утечек информации

Репутационные риски и потери связаны с финансовыми. Они оказывают прямое воздействие на снижение дохода из-за негативного восприятия статуса компании: утрата репутации автоматически влечет упущенную выгоду. Привести к репутационным потерям может утекание сведений, связанных с текущей деятельностью организации, а также данных о каких-то событиях из прошлого. Поэтому нужно уделять внимание защите любых сведений, включая архивные, не использующиеся в данный момент.

Репутационные потери от утечек информации плохо поддаются прогнозированию. Ведь подсчитать, хотя бы приблизительно, сколько клиентов и партнеров откажется от сотрудничества с компанией, невозможно. По подсчетам экспертов более 55% расходов на ликвидацию последствий таких инцидентов в организациях тратятся именно на решение проблем, связанных с репутационным потерями.

Утечка конфиденциальной информации из внутренних источников организации

Оценить уровень мошенничества со стороны сотрудников, динамику масштабов, размеров ущерба, географию и отраслевой ландшафт жертв нарушений, смоделировать портрет нарушителя возможно применяя метод электронного опроса респондентов из числа руководителей и владельцев бизнеса. Так результаты опроса компаний категории «малого бизнеса» (до 100 сотрудников), «среднего бизнеса» (от 500 до 1000 сотрудников), и «крупного бизнеса» (свыше 1000 сотрудников) (рис. 7), проведенного аналитиками «РТК-Солар», указывают на изменения в рабочем поведении рядовых сотрудников и руководителей организаций и связанных с этим внутренних нарушениях в связи с массовым переходом к гибридному режиму работы. Гибридный режим работы подразумевает, что одна часть сотрудников работает на стационарных рабочих местах в офисе, а другая – дистанционно: из дома, а в летние месяцы, возможно, и находясь на даче.

В 2021 году в Трудовом кодексе были детально регламентированы основные процедуры удаленной занятости, в связи с чем соответствующая практика организации труда получила устойчивое распространение в организациях самых разных сфер деятельности.

Удаленка ожидаемо расхолаживает, поддерживать «офисный» уровень контроля, физически находясь с сотрудниками в разных местах, на постоянной основе не под силу практически никому. Соответственно – и вполне ожидаемо – растет и количество самых разных нарушений: и простых дисциплинарных, и таких, которые способны нанести бизнесу значительный урон.

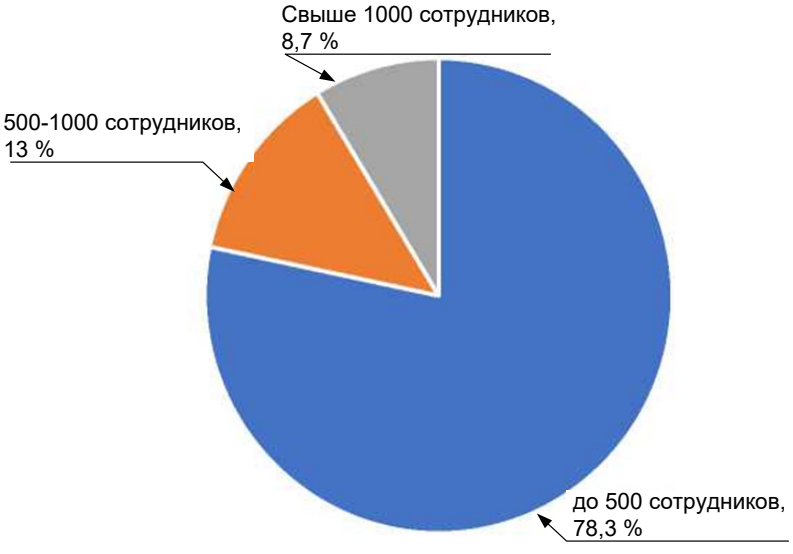


Рисунок 7 – Размер опрошенных компаний

Цифровые следы таких нарушений остаются в корпоративной инфраструктуре.

Из числа респондентов 87 % заявили, что в их организации в 2021 г. имели место случаи мошенничества со стороны сотрудников.

Наиболее часто встречающиеся в российских компаниях виды нарушений – мошеннические действия сотрудников продающих подразделений (почти 20% случаев), различные хищения или предоставление необоснованных преимуществ при закупках (по 14% случаев). Наименее распространенные, экзотические нарушения: кража клиентской базы и данных о клиентах с целью продажи этой информации (примерно в 5% случаев) и хищение разработок компании в целях получения личной выгоды (менее 3% нарушений) (рис. 8).

Основной канал утечки данных в реализации мошеннических схем – это мессенджеры. С их помощью совершена треть нарушений (33%). В половине случаев это различные виды мошенничества с продажами (предоставление безосновательных преимуществ, взяточничество). Именно в мессенджерах реализовывались мошеннические схемы с наибольшим зафиксированным ущербом (рис. 9).

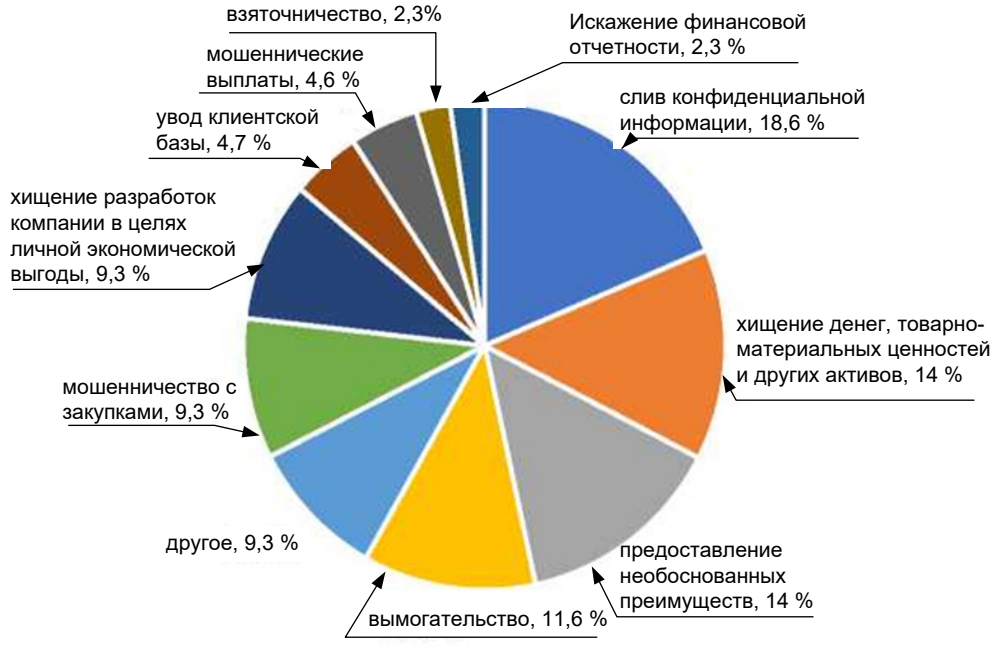


Рисунок 8 – Виды мошенничества, которые допускали сотрудники

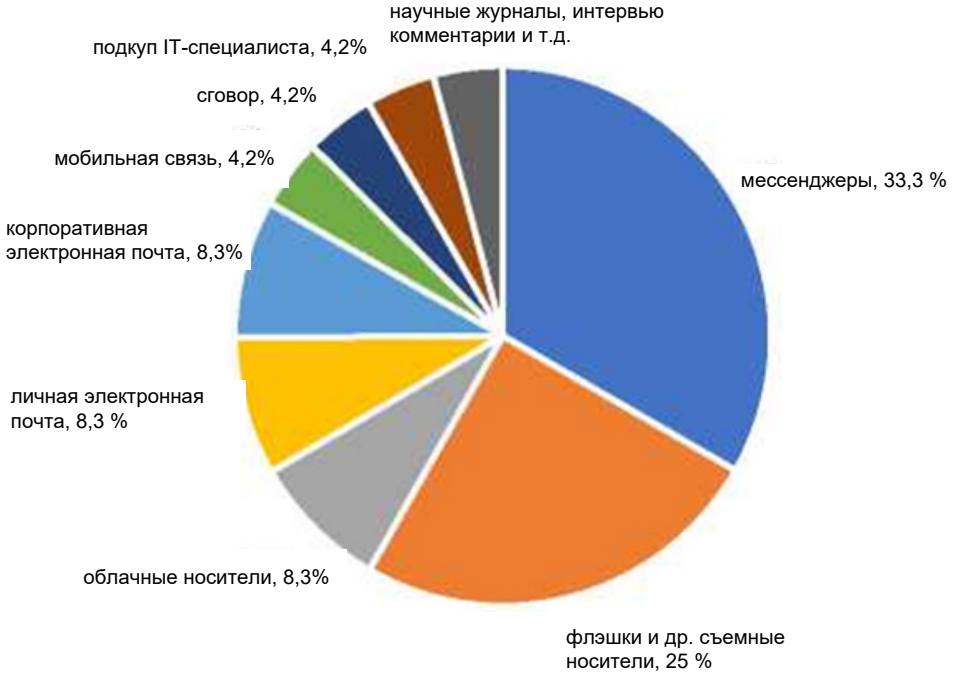


Рисунок 9 – Наиболее частые каналы реализации мошеннических схем

Однозначный лидер среди неблагонадежных подразделений – это отделы продаж (33% инцидентов), далее с большим отрывом следуют производственные подразделения (16,7%), закупки (13%), бухгалтерия и финансы, хранение и логистика (по 10% случаев нарушений) (рис. 10).

Преобладание среди нарушителей сотрудников отделов продаж по сравнению с теми же закупками можно объяснить двумя факторами: общей численностью (как правило, менеджеров по продажам в организациях больше, чем сотрудников закупочных подразделений) и отсутствием четкой законодательной регуляции процедур в сфере продаж, в отличие от закупок.

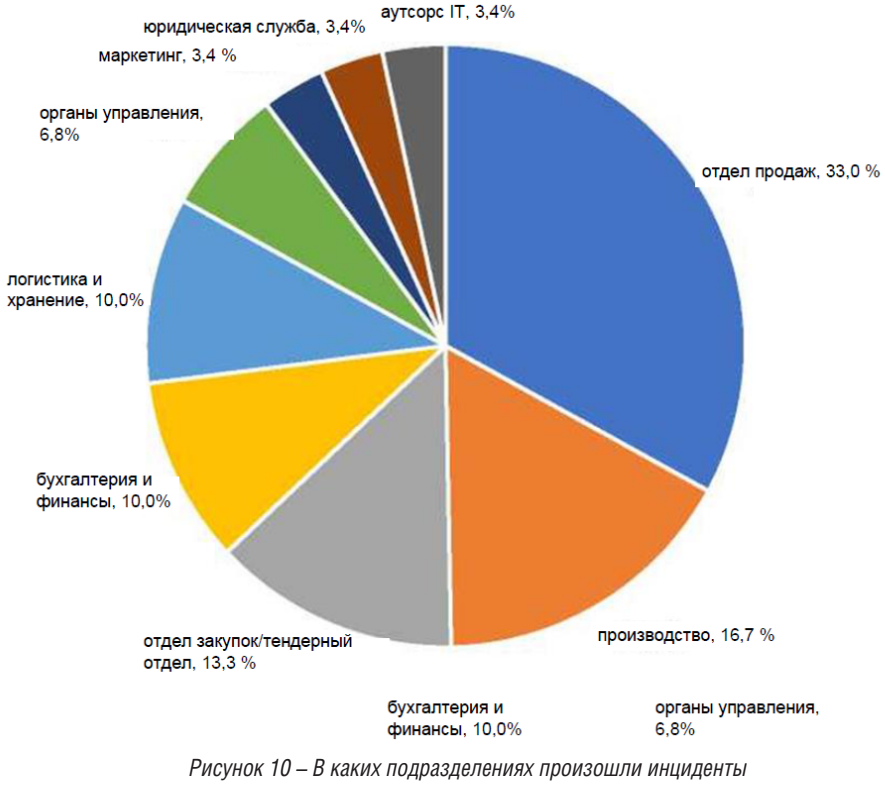


Рисунок 10 – В каких подразделениях произошли инциденты

Подавляющее число нарушений (более 70%) происходит по вине сотрудников среднего возраста (30-50 лет). Лиц старшей возрастной группы (старше 50 лет) вообще нет среди фигурантов нарушений.

Отмечается рост доли умышленных нарушений по вине сотрудников (рис. 11). В 2020 г. доля умышленных нарушений достигла почти 80%. Некоторое снижение в 2021 г., вероятно, связано с повышением латентности внутренних инцидентов, т.е. большая часть их просто остались незамеченными.

Риску инцидентов по утечке конфиденциальной информации с участием сотрудников подвержены самые разные отрасли (рис. 12).

Принимаемые меры для исправления ситуации носили, как правило, характер последействия, а не предупреждения и предотвращения (рис. 13). Только в 8,7% случаев компания принимала решение на использование DLP-системы.

Рисунок 11 – Динамика доли умышленных утечек внутреннего характера: Россия, 2018-2021 гг.

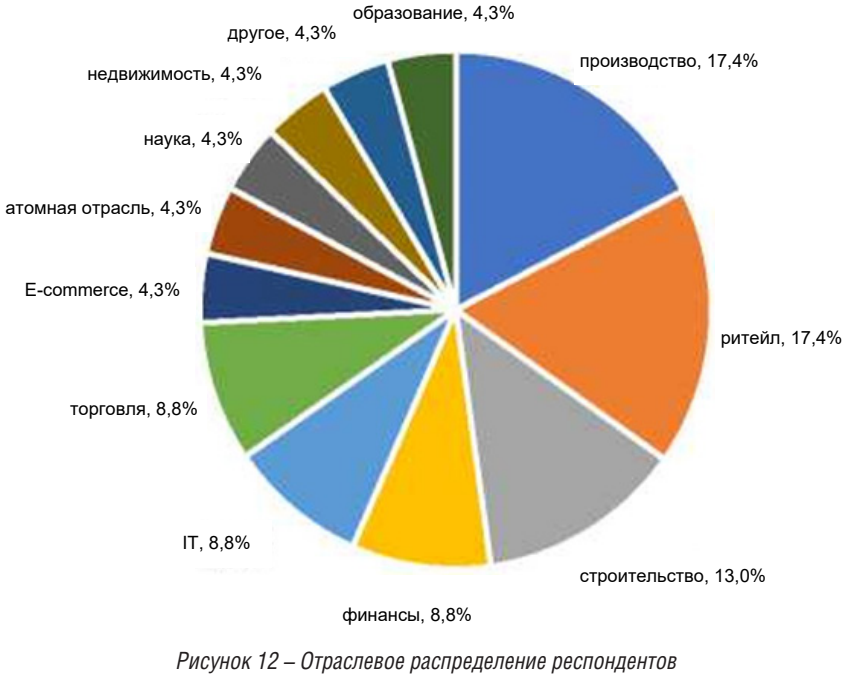


Рисунок 12 – Отраслевое распределение респондентов

Рисунок 13 – Принятые меры для исправления ситуации

Традиционная проблема многих крупных организаций – уровень дисциплины в филиальной сети, который, как правило, существенно ниже центрального аппарата. Запрос на контроль филиальной сети как приоритетная задача встречается почти у каждого крупного заказчика DLP-системы.

Оценка причиненного ущерба от утечек конфиденциальной информации

Суммы причиненного организациям ущерба существенны: почти в 20% случаев его размер составил от 10 до 100 млн. рублей, при этом такой ущерб фиксируют организации среднего размера с численностью сотрудников 500-1000 человек. Приобретение DLP-системы для контроля сотрудников для всей такой организации ориентировочно стоит 10 млн. рублей в год, что соответствует нижнему уровню возможного ущерба.

Наиболее крупный по размеру причиненного ущерба случай мошенничества со стороны сотрудников зафиксирован в крупной (более 1000 сотрудников) производственной организации, базирующейся в одном из отдаленных регионов России. Его размер составил более 100 млн руб. Учитывая, что зафиксированные нарушения имели место в разных подразделениях организации и, скорее всего, происходили на протяжении достаточно длительного периода времени, можно сделать вывод, что в организации с большой вероятностью не использованы никакие инструменты для своевременного выявления подобных ситуаций, в том числе DLP-системы.

Ни один из случаев самых крупных по масштабу нарушений не стал для организаций-жертв поводом для использования ИБ-средств контроля потенциально опасных действий сотрудников. О приобретении DLP-систем по итогам выявленных нарушений сообщили 10% организаций, при этом ущерб во всех был незначительным. Объяснить такую логику можно либо недостаточной осведомленностью высшего руководства организаций о потенциальном решении проблемы в виде DLP-системы, либо отсутствием квалифицированных кадров для её эксплуатации. Хотя данный пробел давно заполняют решения по аналитическому аутсорсингу и возможности вендоров провести качественное обучение inhouse-аналитиков DLP.

При этом ни одна из компаний, для которой мошенничество сотрудников и слив информации вылились в крупный ущерб, в результате не озадачилась внедрением инструментов защиты от утечек. DLP-система пока в основном сфера сугубых интересов служб ИБ, либо ассоциируется система такого класса в основном с борьбой с утечками данных. А низкие размеры штрафов за такого вида нарушения (за исключением, пожалуй, финан-

сового сектора) является слабым мотивом для топ-менеджмента в обеспечении экономической безопасности предприятия.

При этом отечественные DLP-системы по своим функциональным возможностях давно уже перешагнули изначальный, достаточно узкий функционал контроля утечек конфиденциальной информации за пределы организаций. Сейчас они выступают полноценными партнерами и для служб, ответственных за экономическую безопасность, и даже для кадровых служб, которым предлагается набор самых разных метрик: от продолжительности и содержания деятельности на ПК в течение рабочего дня сотрудников до мягкого мониторинга психологического климата в коллективе.

Структуры, подверженные утечке конфиденциальной информации

– утечки данных в госсекторе России:
  • базы данных единого портала Государственных слуг;
  • базы данных Федеральной налоговой службы;
  • Базы данных Пенсионного фонда России;
  • база данных ГИБДД;
  • база данных государственных медицинских учреждений;
  • базы данных государственной системы образования;
  • базы данных силовых структур;
  • база данных Федеральной таможенной службы РФ;
– коммерческие компании:
  • утечки данных из банков России;
  • утечки данных страховых компаний;
  • утечки данных операторов связи;
  • утечки данных торговых сетей;
  • утечки данных из социальных сетей и электронной почты клиентов;
  • утечки данных промышленных предприятий и транспорта;
  • утечки данных ЖКХ.

Утечки данных в социальных сетях

На госструктуры в России приходится 23,3% от общего числа зарегистрированных утечек.

ГИБДД. В 2016 г. произошла утечка данных автовладельцев из ГИБДД. В интернете на бесплатном сервисе autonum.info стало возможным по номеру автомобиля найти имя и номер телефона владельца. Данные с autonum.info можно получить на сайте и по запросу автоинформатору в мессенджере Telegram. Зафиксирована крупная утечка персональных данных российских автовладельцев. По номеру автомобиля на autonum.info в 70-80% случаев находится подлинное имя автовладельца и актуальный номер его мобильного и стационарного телефонов, а также верно определяются и марки автомобилей. Сайт использовал компиляцию баз данных ГИБДД и страховых компаний, а также информацию из открытых источников. Сайт autonum.info зарегистрирован, а сервера находятся в Голландии. Владельцы сервиса неизвестны.

Пенсионный фонд РФ. В 2017 г. Из ПФР утекли данные 17 тысяч человек. ПРФ получил массовую рассылку с прикрепленным документом в формате MS Excel, который содержал данные 17752 человек, в том числе даты их рождения, адреса регистрации и номера СНИЛС. Была ли это целенаправленная деятельность или случайность, установить не удалось.

На портале «Госуслуги» в 2019 г. произошла утечка персональных данных клиентов. В свободном доступе в интернете оказалась информация десятков тысяч пользователей портала «Госуслуги». Персональные данные стали доступны всем желающим в результате утечки.

В Internet в свободном доступе утекла полная таможенная база данных РФ за 2012-2019 годы. Информация содержала все экспортно-импортные операции российских компаний (данные по всем таможенным постам РФ). Данная конфиденциальная информация была выставлена на продажу.

В 2020 г. за крайне высокую цену – в 66,6 биткоина ($627 000) – на продажу была выставлена база данных 115 тыс. возвращавшихся на родину россиян, которая включала сведения: ФИО, дата рождения, паспортные данные, адрес, телефон, e-mail, дата въезда и выезда из России, дата подачи заявления на портале госуслуг, а также данные банковской карты и счета, данные загранпаспорта и страна нахождения.

В период пандемии в Москве был усилен режим передвижения горожан. И в 2020 г. в Dark Web появилось объявление о продаже доступа ко всем камерам видеонаблюдения Москвы, которые установлены на подъездах домов, парковках, в парках, поликлиниках и школах. Покупателю гарантировали доступ к ним в реальном времени, а также к архиву видео за пять дней. Согласно данным столичного Департамента информационных технологий, именно столько времени и хранится информация с камер на территории Москвы. Доступ к данной информации можно было получить всего за 30 тыс. рублей.

Всего за 2020 г. в России зарегистрированы 25 утечек данных заражённых корнавирусом COVID-19. Они коснулись 35,5 тыс. россиян. большинство случаев – это утечки данных отдельных лиц или списков из нескольких десятков или сотен человек. Анализ инцидентов показал, что сфера здравоохранения, погруженная в борьбу с пандемией, не смогла обеспечить защиту основополагающего артефакта цифровой эпохи – персональных данных граждан, включая защищаемую законом информацию о состоянии здоровья. При этом утечки информации о пациентах и о контактных лицах, наносили весьма серьезный удар по людям. Перечни пациентов были сфотографированы и распространены с помощью мессенджеров или групп в соцсетях. Некоторые утечки произошли из-за случайной отправки менеджерами данных на неправильные адреса электронной почты.

В том же 2020 г. произошла утечка паспортных данных участников онлайн голосования по поправкам в Конституцию РФ, включающая паспортные данные, прописку, семейное положение, номера СНИЛС и ИНН, информацию о кредитной истории и т.д. Всего в продаваемую базу данных попали паспортные данные 1,1 млн, использовавших электронную технологию голосования по поправкам в Конституцию РФ.

В России ввели штрафы за принуждение к передаче персональных данных. Закон защищает покупателей, не желающих делиться персональными данными при оплате товаров и услуг. Административная ответственность грозит продавцам услуг в случае отказа заключать, исполнять, изменить или расторгнуть договор с потребителем при его отказе предоставить персональные данные. Закон вступит в силу с 1 сентября 2022 года, устанавливается штраф для должностных лиц в размере от 5 до 10 тысяч рублей, а для юридических — в размере от 30 до 50 тысяч рублей.

Зарубежный опыт

Кибератаки деловой почты в США привели к убыткам в 2021 г. $43 млрд. ФБР и Центр рассмотрения жалоб на интернет-преступления (Internet Crime Complaint Center, IC3) обнаружили, что с июня 2016 года по декабрь 2021 года в результате более 241.000 инцидентов было похищено $43,31 млрд. Взлом служебной электронной почты является прибыльным для киберпреступников.

Мошенничество с компрометацией деловой электронной почты (Business Email Compromise, BEC) позволяет злоумышленнику осуществить несанкционированный перевод средств с помощью взлома служебной или личной учетной записи электронной почты, используя социальную инженерию или компьютерное вторжение. Для достижения своих целей киберпреступники осуществляют кражи личной информации сотрудников, бланки отчетов о заработной плате и налогах (W-2) и криптокошельки.

BEC-атаки часто проводятся с помощью фишинга цели для получения доступа к почтовым ящикам. Злоумышленник ищет важные темы, такие как переписка с поставщиком или с сотрудником внутри компании для дальнейшей атаки на работников или внешнюю компанию.

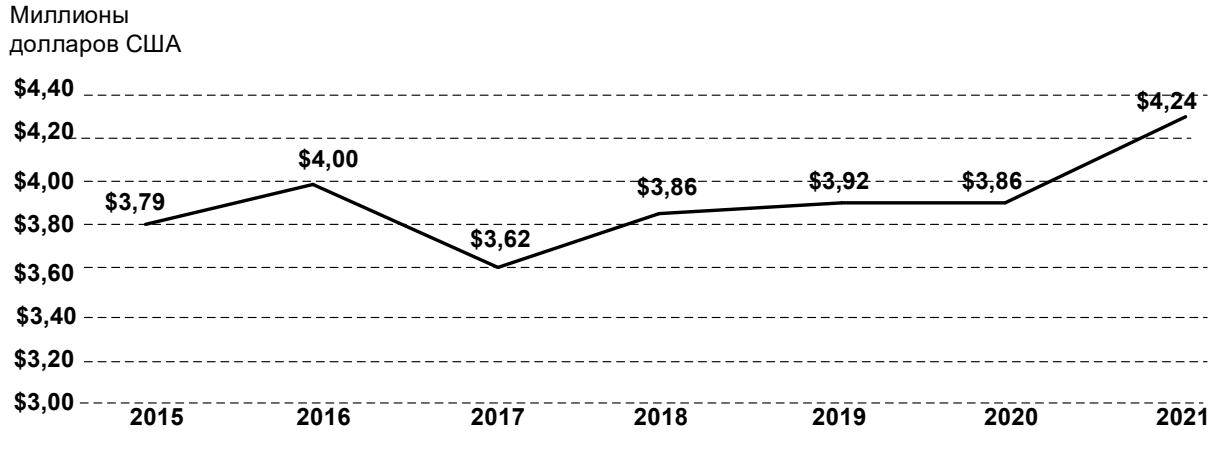
BEC-мошенничество зарегистрировано во всех 50 штатах США и 177 странах мира, причем мошеннические переводы осуществлялись в более чем 140 стран. Основные средства от мошенников проходили через банки Таиланда и Гонконга. Китай, ранее лидирующий в данной сфере, в 2021 году занял третье место, за ним последовали Мексика и Сингапур. У BEC-киберпреступников также была структура поддержки, включающая

наличие денежных мулов[1]. Смурферы передавали отмытые украденные средства мошенникам.

Утечки данных обошлись компаниям в среднем в $4,24 млн. Так например, по оценке IBM Security ущерб от утечек данных в среднем обходится компаниям в $4,24 млн. Это самое высокое значение за 17 последних лет ведения исследований IBM. Глубинный анализ утечек данных более чем в 500 организациях показал, что инциденты в сфере безопасности приводят к возросшим расходам и их сложнее сдерживать, потому что в условиях пандемии кардинально изменились методы работы организаций. Ущерб в 2021 г. по сравнению с 2020 годом увеличился на 10% (рис. 14).

По результатам ежегодного исследования «Cost of a Data Breach Report», проведенного Ponemon Institute при спонсорской и аналитической поддержке IBM Security, были выявлены следующие тенденции в 2021 г.:

– Влияние удаленной работы. Быстрый переход на удаленную работу во время пандемии предположительно увеличил размеры ущерба от утечек данных. В тех случаях, когда одной из причин утечки был признан дистанционный режим работы, ущерб в среднем был на $1 млн. выше, чем в ситуациях, в которых этот фактор не был задействован ($4,96 млн против $3,89 млн).
– Вырос ущерб от утечек в сфере здравоохранения. Отрасли, которым пришлось кардинально изменить подходы к работе во время пандемии (здравоохранение, розничная торговля, гостиничный и ресторанный бизнес, производство и дистрибуция потребительских товаров), также столкнулись с существенным ростом ущерба от утечек данных по сравнению с 2020 годом. Самые дорогостоящие утечки – в здравоохранении: $9,23 млн. на каждый случай, что на $2 млн. больше, чем в 2020 году.
– Компрометация учетных записей приводит к краже данных. Доступ с помощью украденных учетных данных стал причиной большей части утечек, указанных в исследовании. Злоумышленники при этом чаще всего крали персональные данные рядовых пользователей (имя, адрес электронной почты, пароль) – в 44% случаев утечек пострадали данные именно такого типа. Получается движение по спирали: украв имя пользователя и пароль, злоумышленник может в будущем получать доступ к новой информации.



Источник: https://www.ibm.com/downloads/cas/OJDVQGRY

Рисунок 14 – Средняя общая стоимость утечки данных

[1] Денежный мул – это лицо, которое передает (в электронном виде или наличными) полученные от третьего лица деньги другому лицу, получая за это комиссионную плату.

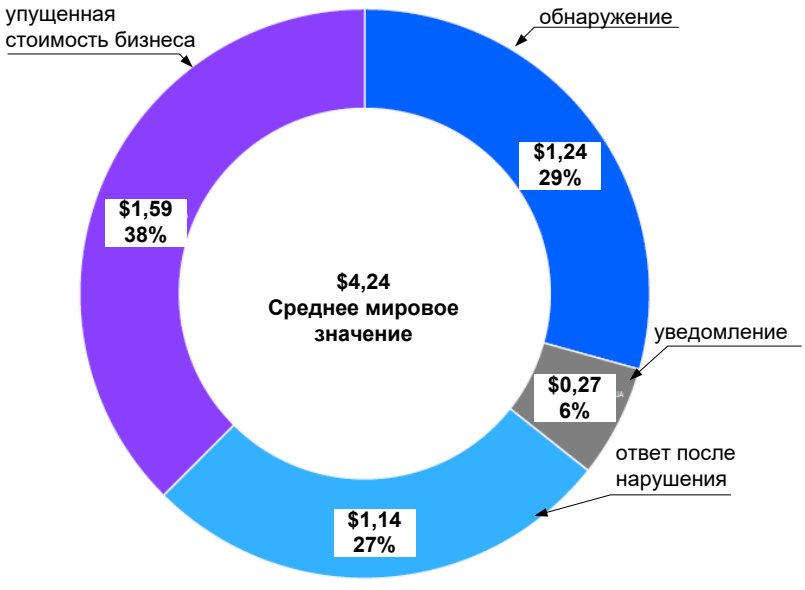


Рисунок 15 – Средняя общая стоимость утечки данных, разделенная на категории

Современные подходы помогают снизить убытки. Применение искусственного интеллекта, ИБ-аналитика и шифрование – три главных фактора, которые доказали свою эффективность в плане уменьшения расходов, связанных с утечками данных. Экономия составила от $1,25 млн. до $1,49 млн. (по сравнению с организациями, где эти инструменты практически не используются). Что касается утечек данных, находящихся в облаке, организациям, применяющим гибридные облака, утечки обходятся дешевле ($3,61 млн.), чем тем, кто использует только публичное облако ($4,80 млн.) или только частное облако ($4,55 млн.).

Более высокие убытки от утечек данных – еще одна статья расходов для бизнеса на фоне быстрого изменения технологий во время пандемии.

Из-за пандемии люди все больше пользуются цифровыми средствами общения. Компании переходили на удаленную работу и облачные технологии, подстраиваясь под реалии.

Отчет показал, что эти факторы существенно влияют на способность компаний реагировать на утечки данных. Почти 20% организаций, принявших участие в исследовании, отметили, что дистанционный режим работы стал одной из причин утечек данных, причем связанные с ним утечки обошлись в 2021 г. организациям в $4,96 млн. (почти на 15% дороже, чем в среднем).

Компании, участвовавшие в исследовании и столкнувшиеся с утечками во время перехода на облачные решения, понесли ущерб, на 18,8% превысивший среднее значение. Однако исследование также показало, что компании, которые дальше других продвинулись по пути модернизации и перехода на работу в облаке (то есть, находились на более «зрелой» стадии), более эффективно выявляли и предотвращали инциденты – в среднем на 77 дней раньше, чем организации, находившееся на начальных стадиях. Исследование случаев утечки данных в облачных инфраструктурах показало, что организациям, применяющим гибридные облака, утечки обходятся дешевле ($3,61 млн), чем тем, кто использует только публичные облака ($4,80 млн) или только частные облака ($4,55 млн).

Отчет также выявил нарастающую проблему: утечки влекут за собой компрометацию данных потребителей (в том числе учетные данные), что в дальнейшем может использоваться для проведения других атак. 82% индивидуальных пользователей, принявших участие в исследовании, признают, что используют одинаковые пароли для разных учетных записей, поэтому компрометация учетных данных является, с одной стороны, основной причиной утечек информации, а с другой, ведет к дальнейшим негативным послед-

ствиям, а значит, представляет собой двойной риск для бизнеса.

- Персональные данные оказываются в руках мошенников. Почти половина (44%) из проанализированных утечек была связана с кражей персональных данных потребителей (имя, адрес электронной почты, пароль и так далее – даже медицинские сведения), и это самый распространенный тип инцидентов в отчете.
- Самый большой ущерб возникает при краже идентифицирующих персональных данных. $180 на каждую украденную запись по сравнению со $161 на каждую запись в среднем по всем категориям утечек.
- Наиболее распространенный метод атаки. Скомпрометированные учетные данные чаще всего использовались как средство для взлома (20% проанализированных утечек данных).
- Более длительное выявление и пресечение. На выявление утечек, причиной которых стала компрометация учетных данных, требуется больше времени – в среднем 250 дней (по сравнению с общим средним показателем – 212 дней).

Некоторые изменения в сфере ИТ во время пандемии увеличили стоимость утечек данных, однако организации, которые не стали модернизировать свой бизнес, на самом деле несут более высокие расходы, связанные с утечками. В организациях, не начавших цифровую трансформацию в связи с COVID-19, ущерб от одной утечки оказался на $750 тыс. выше, чем средний по всем организациям (на 16,6% выше среднего).

Подход «нулевого доверия» помогает компаниям, принявшим участие в исследовании, бороться с утечками данных. Он подразумевает, что любой пользователь в системе или сама сеть могут уже быть скомпрометированы, и использует средства искусственного интеллекта и инструменты аналитики для непрерывной проверки подключений между пользователями, данными и ресурсами. В организациях с развитым подходом «нулевого доверия» ущерб от утечек данных составил в среднем $3,28 млн – на $1,76 млн ниже, чем в компаниях, которые не стали внедрять этот подход.

Также отчет показал, что в 2021 г. больше компаний развернули средства автоматизации защиты по сравнению с прошлыми годами, и это ведет к существенному снижению расходов. Около 65% компаний, принявших участие в исследовании, указали, что они частично или полностью развернули средства автоматизации ИБ – по сравнению с 52% два года назад. В организациях, которые провели развертывание полностью, средний размер ущерба от утечек данных составлял всего $2,90 млн, а у компаний, которые вообще не использовали автоматизацию, тот же показатель оказался выше более чем вдвое – $6,71 млн.

Компаниям, принявшим участие в исследовании, удалось сократить затраты на борьбу с утечкой за счет инвестирования в команды и планы реагирования на инциденты. Организации, создавшие группы реагирования на инциденты и протестировавшие свои планы реагирования, в среднем потратили на ликвидацию последствий взлома $3,25 млн. В то же время компаниям, которые этого не сделали, пришлось потратить в среднем $5,71 млн (разница составляет 54,9%).

Некоторые выводы исследования за 2021 год:

- Время устранения утечек. На то, чтобы выявить и ликвидировать утечку данных, в среднем требовалось 287 дней (212, чтобы выявить, и еще 75, чтобы нейтрализовать) – это на неделю больше, чем в 2020 году.
- Гигантские утечки данных. Средний ущерб в случае гигантской утечки (от 50 до 65 млн записей) составил $401 млн. Это почти в 100 раз больше, чем в большинстве обычных утечек, проанализированных в ходе исследования (от 1 тыс. до 100 тыс. записей).
- Отраслевая специфика. Дороже всего обходились утечки в сфере здравоохранения ($9,23 млн), на втором месте – финансовый сектор ($5,72 млн), на третьем – фармацевтика ($5,04 млн). В сфере розничной торговли, мультимедиа, в гостиничном биз-

несе и общественном секторе ущерб в среднем был ниже, но он тоже заметно вырос по сравнению с 2020 годом.

– Региональная специфика. Самые дорогие утечки происходили в США ($9,05 млн на каждый случай), затем шли страны Ближнего Востока ($6,93 млн) и Канада ($5,4 млн).

Сравнительная характеристика утечки конфиденциальной информации в России, в мире и их тенденция

Анализ статистики утечки конфинедциальной информации в теневых и «полутеневых» ресурсов, таких как платформа Dark web, а также закрытые, анонимные Telegram-каналы показывает возросшее число кибератак с последующими утечками конфиденциальной информации. За первое полугодие 2022 г. (с 1 января по 30 июня 2022 г.) зарегистрировано 2036 утечек. Факт утечки может быть обнаружен как сразу в нескольких источниках (открытых и закрытых), так и только в одном. Фиксируются только умышленные утечки конфиденциальной информации независимо от их «механизма»: кража данных сотрудников или следствие хакерской атаки. На основании объявлений в Dark web и в сетях не представляется возможным определить, кто стал виновников утечки: сотрудник или хакер. С определенной долей вероятности можно предположить, что в основном речь идет о внешнем воздействии хакеров и их подельников. Даже в том случае, если конфиденциальная информация утекла из-за потери физического носителя, такого как USB-флеш-накопитель, или по оплошности сотрудника компании, обнаружение данных злоумышленником и их выставление на продажу переводит такие утечки в категорию умышленных. Анонимно продавать данные может и укравший их сотрудник организации или его сообщник, но количество таких сообщений, следует полагать, значительно меньше. На рисунке 17 представлено распределение обнаруженных утечек данных по странам, где действуют компании и организации, из которых «утекла» информация. Всего обнаружена утечка конфиденциальной информации в 104 странах мира. Для части утечек страна не установлена (9% найденных объявлений о продаже или бесплатном «сливе» данных).

Распределение по топ-11 странам выглядит следующим образом:

США – 30%; РФ – 13%; Великобритания/Германия/Индия/Канада/ – по 3%; Бразилия/Испания/Италия/Китай/Украина/Франция – по 2% (рис.16).

Рисунок 16 – Число объявлений о продаже данных

Регулярно первое место по количеству утечек занимают США. Поэтому не является исключением и мониторинг утечек в Dark web и закрытых Telegram-каналах. Такое положение вполне объяснимо: США все еще обладают самой мощной экономикой мира, именно здесь зарегистрированы сотни корпораций, ряд из которых оперируют данными миллиардов людей и обладают очень ценными ноу-хау.

На втором месте – Российская Федерация, число кибератак на информационные ресурсы которой существенно возросло с марта 2022 г., что привело к большему, чем в аналогичном периоде 2021 года, числу утечек конфиденциальной информации.

На рис. 17 представлено отраслевое распределение утечек из компаний и организаций по всему миру, чьи данные оказались в Dark web.

Больше всего (19%) объявлений о продаже данных относилось к промышленным и транспортным компаниям, включая как пассажирские перевозки, так и грузовые. На втором месте (16%) – объявления о продаже данных высокотехнологичных компаний, а на третьем – торговых сетей (15%).

Если сравнить распределение утечек в Dark web по отраслям организаций в мире (рис. 17) и в России (рис. 18), то окажется, что распределения во многом очень похожи.

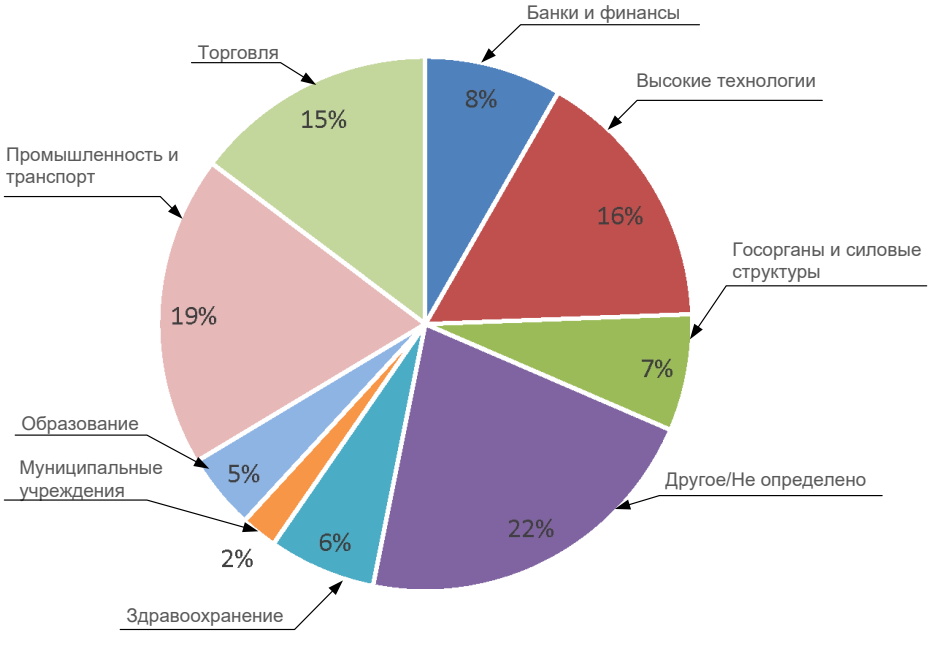


Рисунок 17 – Распределение утечек в Dark web по отраслям организаций в мире

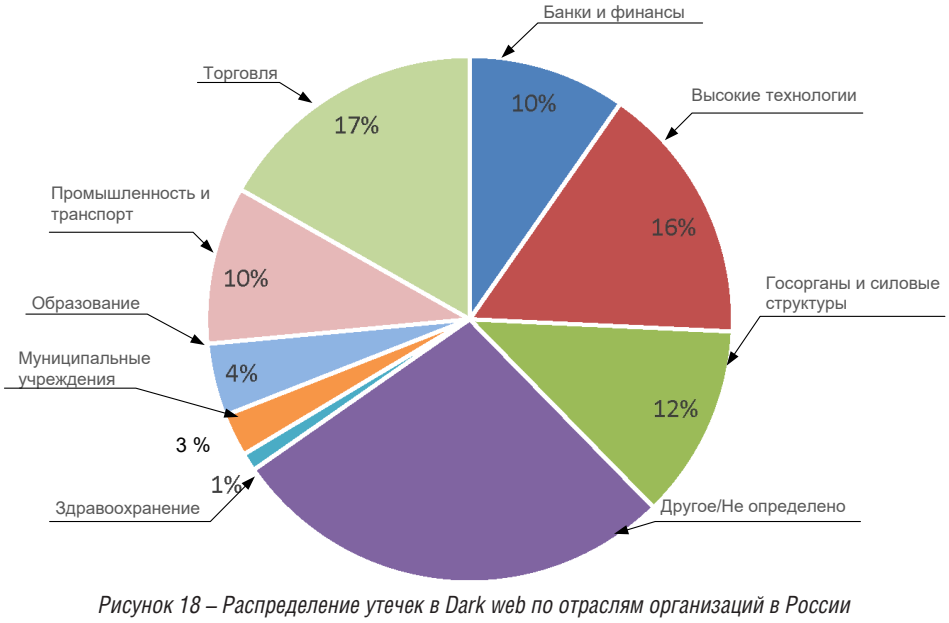


Рисунок 18 – Распределение утечек в Dark web по отраслям организаций в России

За исключением нескольких аспектов:

1. В России доля утечек, которые пришлись на организации сферы «Торговля» несколько выше, чем в мире – 27% против 22%. По-видимому, хакеры в последнее время испытывали повышенный интерес к масштабным клиентским базам крупных российских ритейлеров и поставщиков услуг.

2. Доля утечек из промышленных и транспортных организаций в России (10%) оказалась ниже, чем в мире (19%).

Значительнее всего отличаются доли утечек информации в высокотехнологичных компаниях: если в мире на такие компании приходится 19,7% утечек от общего количества, то в Dark web доля составляет 16%. Еще больше различия обнаруживаются, если рассматривать распределения утечек в секторе «Высокие технологии» в России: доля утечек от общего количества – 27,9%, а в объявлениях в Dark web – 16%.

Можно предположить, что целью хакеров при кибератаках в меньшей степени являются компании этого сегмента рынка. Такая же картина наблюдается и для организаций сферы «Здравоохранение». Но если рассматривать промышленные и транспортные компании, то ситуация обратная. В мире (19%) и России (10%) чаще хакеры выкладывали объявления о продаже или передаче данных в Dark web. В общем числе утечек информации доли в мире и России составили 14,4% и 7,5%, соответственно. Как в глобальном масштабе, так и в России есть внушительная часть случаев, когда отраслевую принадлежность пострадавшей компании либо невозможно отнести ни к одной из обозначенных категорий, либо вообще нельзя определить. В общем количестве утечек доля случаев категории «Другое/не определено» составляет 22% в мире и 16,7% в России, среди утечек из Dark web – 22% в мире и 27% в России (табл. 1). Такое значительное увеличение доли утечек в организациях «неопределенной отрасли» объясняется тем, что зачастую в объявлениях не уточняют происхождение данных, предлагают приобрести базу «персональных данных россиян», «паспортов россиян» и т.д.

Интерес к конфеденциальной информации зависит от размеров самой организации. Пострадавшие компании и организации по размеру: маленькие (<50 сотрудников), средние (<500 сотрудников) и крупные (>500 сотрудников) показаны на рис. 19.

Сравнительный анализ утечки конфиденциальной информации указывает на то, что в Dark web в первом полугодии 2022 г. в основном продавали данные организаций среднего сегмента – 46%. Но при этом значительно котируется информация крупных компаний – 30%. Порой (16% случаев) не удается установить размер организации, в которой произошла утечка данных. Схожее распределение мы наблюдаем и в России за исключением того, что доля организаций, для которых не установлен их размер, выше – 24% в России против 16% в мире.

По содержанию продаваемой информации в Dark web и на специализированных Telegram-ка-

Таблица 1 – Сравнение утечек, выявленных в Dark web, со сводным количеством утечек, выявленных из различных источников

	Общая база		Утечки в Dark web	
	Мир	Россия	Мир	Россия
Банки и финансы, %	7,3	8,5	8	10
Высокие технологии, %	19,7	27,9	16	16
Госорганы и силовые структуры, %	8,6	10,5	7	12
Другое/Не определено, %	22,2	16,7	22	27
Здравоохранение, %	7,2	2	6	1
Муниципальные учреждения, %	3,1	3,6	2	3
Образование, %	5	5,6	5	4
Промышленность и транспорт, %	14,4	7,5	19	10
Торговля, %	12,5	17,7	15	17

налах приоритет отдается (в 81% случаях) базам персональных данных клиентов компаний и государственных органов. В 13% случаев речь идет о продаже коммерческих тайн компаний, а 3% и 2% объявлений, соответственно, предлагают платежную информацию и сведения категории «государственная тайна» (рис. 20).

И в мире, и в России основной целью хакеров остаются персональные данные: 81% инцидентов относятся к персональным данным в мире и 60% в России.

Доля украденных коммерческий тайн в России в распределении выше, чем в мире: 21% против 13%. Это может быть связано с кибервойной, проводящейся против организаций, формирующих российскую экономику. Две самые крупные с точки зрения числа скомпрометированных уникальных записей персональных данных утечки данных в мире – это утечка из бразильской компании-разработчика платежного инструмента (66 миллионов записей) и утечка пользователей онлайн-сайта для взрослых (65 миллионов записей).

Встречаются в теневой Сети и совсем небольшие базы, содержащие около 1000 записей. При сравнительном анализе распределения утечек из объявлений в Dark web с распределением общего количества утечек можно отметить, что превали-

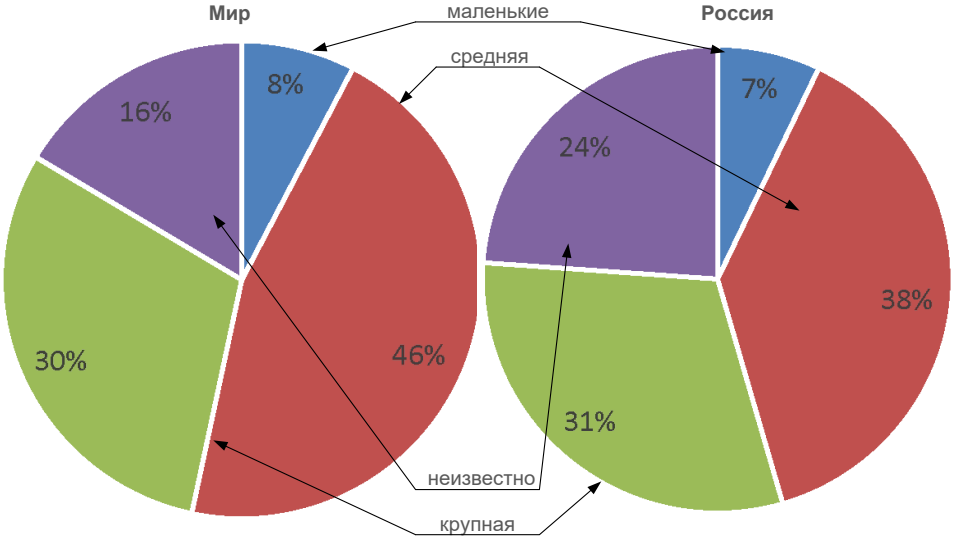


Рисунок 19 – Распределение утечек из объявлений в Dark web по размеру организаций

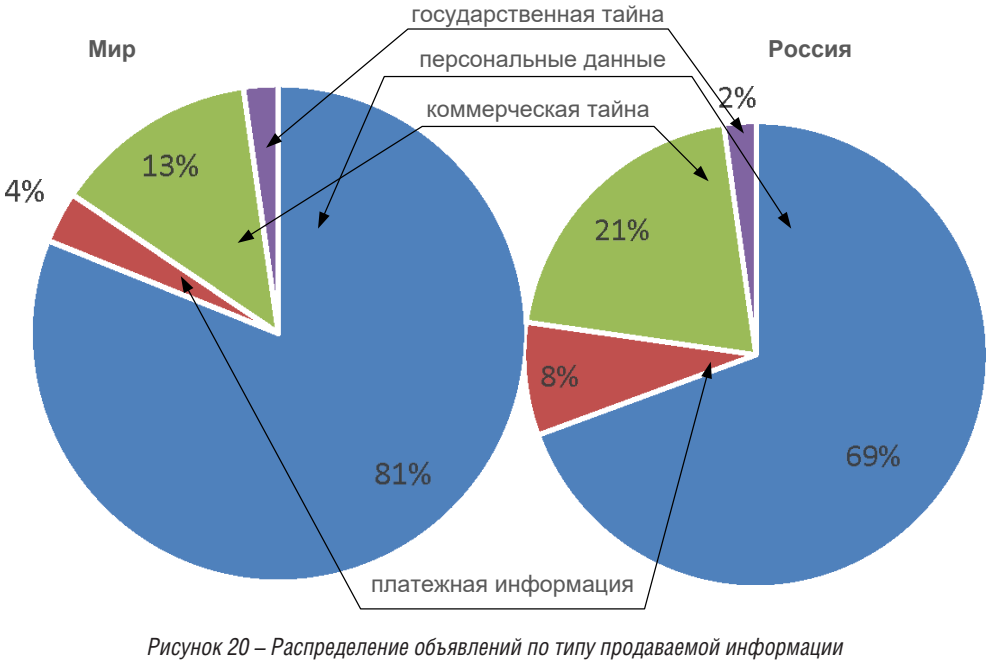


Рисунок 20 – Распределение объявлений по типу продаваемой информации

рующая доля утечек в обоих случаях относится к персональным данным – в мире 82,9% в общем распределении, 81% в распределении утечек в ДаркВебе. На втором месте утечки, связанные с кражей коммерческих тайн компаний: в мире 13,4% в общем распределении и 13% в распределении утечек в Dark web. В обоих источниках также невелика доля утечек сведений, составляющих государственную тайну, – порядка 2%. Доля утечек из объявлений в Dark web, пришедшихся на платежную информацию, составляет 4% в мире. В общем распределении эта выборка несколько теряется и составляет уже 1,5%. А в России в объявлениях о продаже или бесплатной передаче данных платежная информация встречается достаточно часто – в 8% случаев. В общем распределении это значение снова теряется – всего 0,7%

Выводы

С учетом происходящих событий на глобальном и региональном уровне интенсивность утечек конфиденциальной информации будет возрастать как в мире, так и в России. В рамках гибридной войны, включающей в себя как применение летального оружия, разрушения инфрасруктуры, вооружения и военной техники, так и экономическое противодействие, информационную войну и воздействие на ментальность людей, несомненно будет возрастать интенсивность кибервойн, уибератак, широкое распространение хакерских инструментов и повышение значимости информации в мире, а также стремление ее использовать как инструмент шантажа, экономического и политического давления.

Возрастает латентность внутренних нарушений. Если в компании нет на вооружении современных инструментов защиты от действий персонала, службам безопасности крайне затруднительно проводить мероприятия по выявлению инцидентов и в сборе доказательной базы для проведения расследований. Ситуация осложняется тем, что вектор многих атак становится все более сложным, злоумышленники из-за пределов информационного контура организации все чаще вступают в сговор с сотрудниками и реализуют многоступенчатые схемы похищения информации. Обращает на себя внимание тот факт, что значительно выросла доля утечек коммерческой тайны. Наибольшее давление злоумышленников в I полугодии 2022 г. испытывали производственные компании, в том числе связанные с оборонным сектором. От кражи персональных данных чаще всего страдал ритейл и высокотехнологические компании.

Анализ статистики о продаже данных в Dark web позволяет сделать вывод о процветании этого сегмента: ежедневно на подпольных форумах появляются десятки объявлений о продаже свежих баз данных, также злоумышленники предлагают (зачастую бесплатно или за символически деньги) базы из утечек прошлых лет. Усилия правоохранительных органов пока не дают ожидаемого эффекта – закрытие крупнейшей хакерской торговой площадки RaidForums. Ввод оборотных штрафов может повлиять на отношение к обеспечению безопасности персональных данных и к задачам специалистов по информационной и экономической безопасности.

Список литературы

1. *Матвеев А.В., Матвеев В.В.* Системно-кибернетический подход к определению понятия «безопасность» // Национальная безопасность и стратегическое планирование. – 2015. – № 1(9). – С. 18-25. – EDN THRQRD.

2. *Зайцев А.К., Матвеев В.В.* Экономические преступления с использованием цифровых технологий // Национальная безопасность и стратегическое планирование. – 2022. – № 1 (37). – С. 63-81. – DOI 10.37468/2307-1400-2022-1-63-81. – EDN WFNIFZ.

3. *Матвеев В.В., Филатова Т.А.* Методы управления организационными системами в условиях риска и неопределенности с целью обеспечения экономической безопасности // Национальная безопасность и стратегическое планирование. – 2021. – № 2 (34). – С. 73-96. – DOI 10.37468/2307-1400-2021-2-73-96. – EDN FVOOLC.

4. *Андрианов, В.В.* Обеспечение информационной безопасности бизнеса / В.В. Андрианов. – М.: Альпина Паблишер, 2020. – 759 с.

5. *Матвеев А.В., Матвеев В.В.* Методологические основы объединения социально-экономических систем в условиях глобализации (на примере ЕАЭС) // Национальная безопасность и стратегическое планирование. – 2017. – № 2-2 (18). – С. 187-208. – EDN ZQLGFL.

6. Россия. Утечки информации ограниченного доступа в 2021 году. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/products/zaschita-asu-tp-arma/kiberbezopasnost-asu-tp-console

7. InfoWatch Vision визуализирует данные DLP-системы Traffic Monitor в виде статистики и графа связей. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/products/vision

8. *Варлатая С.К., Шаханова М.В.* Криптографические методы и средства обеспечения информационной безопасности. Учебное пособие. – М.: Проспект, 2019. – 152 с.

9. Россия. Утечки информации ограниченного доступа в 2021 году. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/

10. *Гайсина А.Р., Матвеев В.В.* Противоречие реализации судебных принципов в деятельности процессуальных участников как лишение возможностей содействия правосудию // Национальная безопасность и стратегическое планирование. – 2022. – № 1(37). – С. 97-105. – DOI 10.37468/2307-1400-2022-1-97-105. – EDN TXZVUF.

11. Исследование «Мошенничество и слив данных в российских организациях» Апрель-май 2022. [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/upload/iblock/9e4/wbe0s6mkqyd09ymydi3l80pv688yhfml/RTK_Solar_-issledovanie-Moshennichestvo-i-slivy-dannykh-v-rossyskikh-kompaniyakh.pdf

12. Система предотвращения утечек информации (DLP). [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/products/solar_dozor/

13. *Грошева Е.К., Невмержицкий П.И.,* Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний. – 2017. – № 3. – С. 36.

14. Информационная безопасность: Учебное пособие / Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

15. Атаки на российские компании в 2022 г. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/products/vision

16. *Бородушко И.В., Матвеев В.В.* 3.1. Экономическая безопасность в условиях цифровой трансформации социально-экономических систем в Российской Федерации // В книге: Экономическая безопасность в новой реальности. Санкт-Петербург, 2021. – С. 113-126. – EDN QHQOXB.

17. *Шаньгин В.Ф.* Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: Форум, 2018. – 256 с.

Статья поступила в редакцию 26 июня 2022 г.
Принята к публикации 6 сентября 2022 г.

Ссылка для цитирования: Гайсина А.Р., Зайцев А.К., Матвеев В.В. Обеспечение экономической безопасности при утечке конфиденциальной информации // Национальная безопасность и стратегическое планирование. 2022. № 3(39). С. 52-75. DOI: https://doi.org/10.37468/2307-1400-2022-3-52-75

For citation: Gaysina A.R., Zaitsev A.K., Matveev V.V. Ensuring economic security in case of leakage of confidential information // National security and strategic planning. 2022. № 3(39). pp. 52-75. DOI: https://doi.org/10.37468/2307-1400-2022-3-52-75

Сведения об авторах:

ГАЙСИНА АЛИНА РИНАТОВНА – *студент кафедры экономической безопасности Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Россия*
e-mail: alinagaysina020401@gmail.com

ЗАЙЦЕВ АЛЕКСАНДР КОНСТАНТИНОВИЧ – *аспирант кафедры экономической безопасности Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Россия*
e-mail: alexanderzaitsev619@gmail.com

МАТВЕЕВ ВЛАДИМИР ВЛАДИМИРОВИЧ – *доктор технических наук, кандидат экономических наук, профессор, профессор кафедры экономической безопасности Санкт-Петербургского государственного экономического университета, первый вице-президент Петровской академии наук и искусств действительный член Академии военных наук, г. Санкт-Петербург, Россия*
e-mail: 070355mvv@ gmail.com

Information about authors:

GAYSINA ALINA R. – *Student of the Department of Economic Security, St. Petersburg State University of Economics, St. Petersburg, Russia*
e-mail: alinagaysina020401@gmail.com

ZAITSEV ALEXANDER K. – *Postgraduate student of the Department of Economic Security, St. Petersburg State University of Economics, St. Petersburg, Russia*
e-mail: alexanderzaitsev619@gmail.com

MATVEEV VLADIMIR V. – *Doctor of Technical Sciences, Candidate of Economic Sciences, Professor, Professor of the Department of Economic Security, St. Petersburg State University of Economics, First Vice-President of the Petrovsky Academy of Sciences and Arts, Full member of the Academy of Military Sciences, St. Petersburg, Russia*
e-mail: 070355mvv@ gmail.com