Исследование утечек информации ограниченного доступа в 2020 году

Оглавление

Оглавление 2

Только факты 3

Сокращения 4

Аннотация 4

Результаты исследования 5

- Динамика количества утечек и количества утекших записей 5
- Крупных утечек стало больше 8
- Рост доли инцидентов внешнего характера 9
- Хакерские атаки вышли на первый план 13
- Платежные данные все сложнее монетизировать, но более ликвидными на черном рынке становятся ПДн 15
- Доля прямого мошенничества с «утекшими» данными сократилась 16
- США: выявленных утечек стало существенно меньше 18
- Каналы утечек 18
- Распределение по отраслям 23

Исследование инцидентов ИБ, связанных с действиями увольняющихся сотрудников 25

Заключение 30

Мониторинг утечек на сайте InfoWatch 31

Методика 31

Глоссарий 35

Только факты

- ✓ В 2020 году специалистами Экспертно-аналитического центра InfoWatch зафиксировано **2395** утечек данных из коммерческих, некоммерческих (государственных, муниципальных) организаций в различных странах мира. Это на **4,5%** меньше, чем в 2019 году (2509 утечек), но на 5,8% превышает показатели 2018 года (2263).
- ✓ За 2018-20 гг. **сохраняются тенденции роста** доли **утечек умышленного характера** (внешних и внутренних) и **снижения** доли **утечек внутреннего характера**.
- ✓ Общая доля умышленных утечек **ПДн** выросла с **60,2%** до **72,5%**.
- ✓ Доля утечек **платежной информации** (как умышленных, так и неумышленных) продолжает падать, в 2020 г. по сравнению с 2019 г. она сократилась в 2 раза, по сравнению с 2018 – более чем 3 раза.
- ✓ **55,9%** утечек были спровоцированы внешними нарушителями, **44,1%** - внутренними.
- ✓ **35,4%** утечек стали результатом действий и бездействия непривилегированных сотрудников.
- ✓ Более **11 млрд** записей ПДн и платежной информации оказалось скомпрометировано за прошлый год, что по сравнению с 2019 годом снизилось более чем на 25%.
- ✓ **4,62 млн** записей в среднем было скомпрометировано в результате одной утечки. Это на 22% меньше, чем в 2019 году.
- ✓ В 2020 году было зафиксировано **84** утечки, в результате каждой из которых «утекло» более **10 млн** записей. Совокупно на такие разрушительные утечки пришлось **95,7%** всех скомпрометированных записей.
- ✓ В общей совокупности утечек с числом утекших записей менее 1 млн каждая, в 2020 году на каждую утечку в среднем пришлось **28,1 тыс.** записей, тогда как в 2019 году на подобную утечку в среднем приходилось **19,9 тыс.** записей.
- ✓ В 2020 году **2,8 млн** записей в среднем пришлось на утечку внешнего характера, **6,8** млн записей – на утечку внутреннего характера.
- ✓ Более **79% утечек** происходит через Сеть[1].
- ✓ Доля утечек с использованием электронной почты и бумажных документов в течение 2018-20 гг. продолжает падать.

[1] См. Глоссарий

Сокращения

GDPR	General Data Protection Regulation (Регламент Евросоюза о персональных данных от 27.04.2016 г., вступил в силу 25.05.2018 г.)
ИБ	Информационная безопасность
ИС	Информационная система
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ЭАЦ	Экспертно-аналитический центр ГК ИнфоВотч

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch (далее ЭАЦ) представляет ежегодное исследование утечек информации ограниченного доступа. В 2020 году главным мировым событием стала пандемия новой коронавирусной инфекции. Борьба с опасным вирусом радикально повлияла на ключевые процессы, заставила изменить многие привычные формы предоставления услуг и привела к экономическим трудностям в разных регионах. Естественно, такой мощный фактор как пандемия не мог не повлиять на сферу информационной безопасности. В этом исследовании мы рассказываем о том, как за год изменилась структура утечек информации.

Может показаться странной ситуация с уменьшением количества и общего объёма утечек по сравнению с предыдущим годом, несмотря на ослабление контроля за обращением данных, вызванного массовым переходом на удалённую работу вследствие пандемии COVID-19.

Тем не менее, посмотрев на ситуацию даже за 3 последних года, мы увидели, что идёт рост количества умышленных утечек, персональных данных и коммерческой тайны, увеличение доли сетевого канала и снижение роли бумажных документов.

Авторы попытались выявить и обозначить наиболее значимые тенденции, которые позволили бы специалистам-практикам из сферы ИБ найти пути решения ряда проблем защиты информации при выходе из режима пандемии и возвращения к привычному ритму деловой активности.

Авторы отчета уверены, что результаты исследования будут интересны специалистам в области информационной и экономической безопасности, журналистам, собственникам и высшему менеджменту компаний, которые работают с информацией ограниченного доступа (например, сведениями, составляющими коммерческую, банковскую, налоговую тайну).

Результаты исследования

Динамика количества утечек и количества утекших записей

В 2020 году Экспертно-аналитическим центром InfoWatch зарегистрировано (стали известными) **2 395**[2] случаев утечки информации ограниченного доступа из коммерческих компаний, государственных органов и организаций. Это на 4,5% меньше, чем годом ранее, но на 5,8% превышает показатель 2018 года (Рисунок 1).

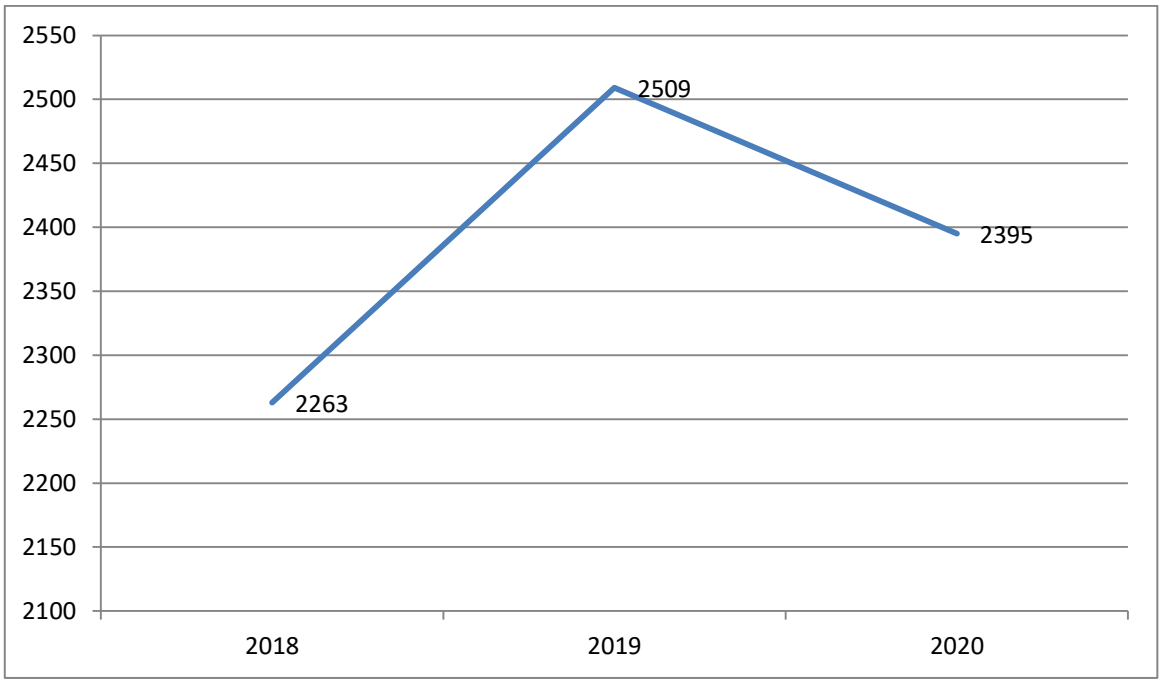


Рисунок 1. Число утечек информации, 2018 - 2020 гг.

В результате утечек, информация о которых стала достоянием общественности за год, оказались скомпрометированы 11,06 млрд записей персональных данных и платежной информации (далее – пользовательская информация), в частности, имена и фамилии, адреса электронной почты, номера телефонов, пароли, сведения о постоянном месте жительства, номера социального страхования, реквизиты банковских карт и данные о банковских счетах (Рисунок 2).

[2] В ряде отчетов встречается значение порядка 4000, но там речь идёт о нарушениях (breaches) и необходимо понимать, что не каждое нарушение порядка работы с информацией ведёт к утечке.

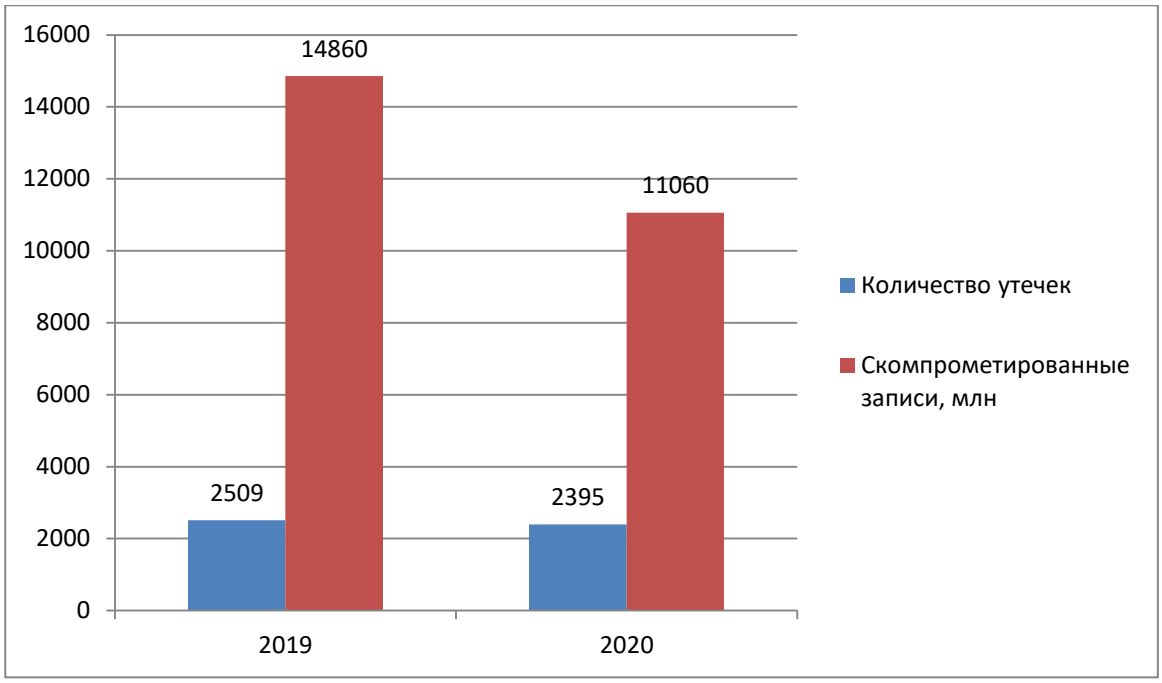


Рисунок 2. Число утечек информации и объем персональных данных, скомпрометированных в результате утечек. 2019 - 2020 гг.

Bleeping Computer: Киберпреступники из группировки ShinyHunters взломали популярное сообщество Wattpad, объединяющее авторов и любителей книг. По данным компании Cyble, сведения более 270 млн подписчиков Wattpad предлагались в Даркнете за 10 биткойнов (почти $100 тыс.), но через некоторое время стали распространяться бесплатно. Подпольный дилер уверяет, что в базе почти 200 млн паролей, из которых 145 млн зашифрованы с помощью довольно надежного алгоритма bcrypt, а 44 млн имеют относительно слабую криптозащиту SHA256. Образцы данных, изученные журналистами, содержали имена пользователей, реальные имена, хэшированные пароли, адреса электронной почты и географические координаты.

Таким образом, общее число скомпрометированных записей по сравнению с 2019 годом снизилось на 25,5% - с 14 ,86 до 11,06 млрд. В результате средний размер утечки снизился на 22% - с 5,92 млн записей в 2019 г. до 4,62 млн записей в 2020 году

Как видно из рисунка выше, в 2019 г. произошел резкий скачок количества скомпрометированных записей – 7,19 млрд до 14,86 млрд, в 2020 г. зафиксировано падение их количества более чем на четверть – до 11,06 млрд.

Далее рассмотрена динамика количества скомпрометированных записей персональных данных и платежной информации за последние три года — с 2018 по 2020 год.

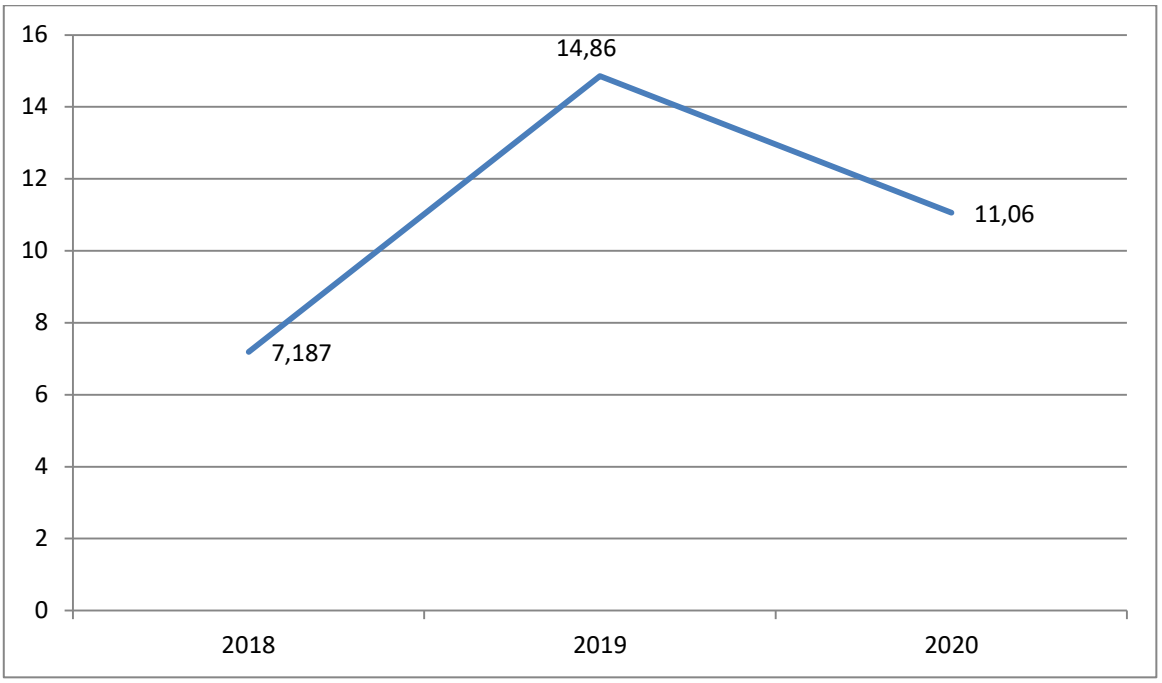


Рисунок 3. Количество скомпрометированных записей ПДн и платежной информации, млрд, 2018 - 2020 гг.

На наш взгляд, падение количества зарегистрированных (опубликованных) утечек прежде всего связано с повышенным уровнем латентности инцидентов в период пандемии. Спешно перестраивая формы реализации многих процессов, массово переводя сотрудников на дистанционную работу, весной 2020 года далеко не все компании успели оперативно адаптировать системы информационной безопасности к новым реалиям. ***При этом нельзя забывать, что значительная часть случаев утечек становится достоянием общественности далеко не сразу после инцидентов, а только после публикации утекших данных в открытом доступе или в результате их продажи. В результате еще больший процент утечек, чем раньше, мог оставаться в «серой зоне».***

Снижение на четверть общего объема скомпрометированных записей ПДн и платежной информации объясняется снижением количества зафиксированных в Сети случаев распространения гигантских баз данных, включающих по миллиарду записей и более. К тому же, эти сборники данных неизвестные лица в основном составляли на основе данных из гигантских утечек прошлых лет: Yahoo, Experian, Equifax, Facebook. Вероятно, потенциал использования этих данных на черном рынке уже исчерпан, а огромные базы из утечек последнего времени еще не успели попасть в широкий «оборот».

Любой подобный пример кардинальным образом влияет на общую картину.

Хотя эти базы, как правило, формируются на основе украденных данных в результате не одного инцидента, а целого ряда утечек разных лет, мы считаем правильным принимать во внимание подобные «сборники» и включать их в общую статистику. ***В этих базах встречаются данные, полученные в результате ранее не зафиксированных утечек, в т.ч. произошедших вследствие компьютерных***

атак. Кроме того, передавая данные по цепочке, продавцы в даркнете могут обогащать их новыми записями. Это замечание относится и к характеристикам более мелких баз, распространяемых на черном рынке. Если в 2019 г. из отрытых источников стало известно о распространении четырех гигантских баз с числом записей от 1 млрд, то в 2020 г. таких примеров было только два.

Крупных утечек стало больше

Несмотря на сокращение как количества утечек, так и общего количества скомпрометированных пользовательских записей, в 2020 году стало больше крупных утечек, в результате каждой из которых было скомпрометировано не менее 1 млн записей. Если в 2019 году таких утечек было 169, то в 2020 году их зафиксировано 213 (рост на 26%). Выросло и число «мега-утечек» - инцидентов, в результате каждого из которых было украдено или случайно скомпрометировано более 10 млн. записей ПДН и (или) платежной информации. В 2020 г. ЭАЦ зарегистрировал 84 «мега-утечки» - на 12 больше, чем годом ранее (рост на 16,6%).

На случаи «мега-утечек» в 2020 году пришлось 10,59 млрд утекших пользовательских записей или 95,7% от совокупного объема данных, скомпрометированных за год. За 2019 год авторы исследования в результате «мега-утечек» насчитали 14,4 млрд скомпрометированных записей или 97,1% от совокупного объема данных, скомпрометированных в 2019 году.

Без учета утечек объемом свыше 1 млн записей, в 2020 году на каждую утечку в среднем пришлось 28,1 тыс. записей, тогда как в 2019 году на подобную утечку в среднем приходилось 19,9 тыс. записей.

То есть «типичная» утечка в среднем «потяжелела» примерно на 41,2%. Кстати, в 2019 г. средняя утечка объемом менее 1 млн записей «прибавила в весе» около 43% по сравнению с 2018 г. Поэтому интересно будет посмотреть, сохранится ли такая динамика в 2021 г.

По мнению авторов исследования, наметившийся в последние годы рост среднего объема записей в расчете на утечку (без учёта многомиллионных утечек, которые сильно влияют на общую статистику) объясняется динамичным развитием цифровизации, предоставлением широкого спектра услуг в электронном виде. Как государственные организации, так и коммерческие компании накапливают большие объемы информации о гражданах, утечки даже из небольших компаний могут приводить к компрометации десятков и сотен тысяч записей ПДн. Компании также все активнее пользуются услугами поставщиков различных услуг и доверяют им клиентские данные. Естественно, это создает новые риски информационной безопасности, и далеко не все научились управлять этими рисками.

> *EDPB: В Нидерландах местное управление по защите данных (Autoriteit Persoonsgegevens, AP) выписало штраф Королевской голландской теннисной ассоциации (KNLTB). Регулятор выяснил, что ассоциация сливала персональные*

данные своих участников. По данным AP, менеджеры KNLTB передавали личную информацию участников двум компаниям-спонсорам. В первом случае речь идет о персональных данных 50 тыс. членов ассоциации, во втором — о данных более 300 тыс. членов. Незаконно отправленные данные включают имена, гендерную принадлежность и адреса. Такая информация была довольно ценной для спонсоров — благодаря ей они могли обращаться к участникам KNLTB с рекламными предложениями, связанными с темой тенниса. AP выяснило, что многие граждане получали подобные предложения по телефону и электронной почте.

Рост доли инцидентов внешнего характера

В 2020 году основной вектор утечек продолжал смещаться в сторону внешнего нарушителя (Рисунки 4-5). Действия хакеров и неизвестных лиц из-за пределов информационного контура организаций привели к 55,9% утечек.

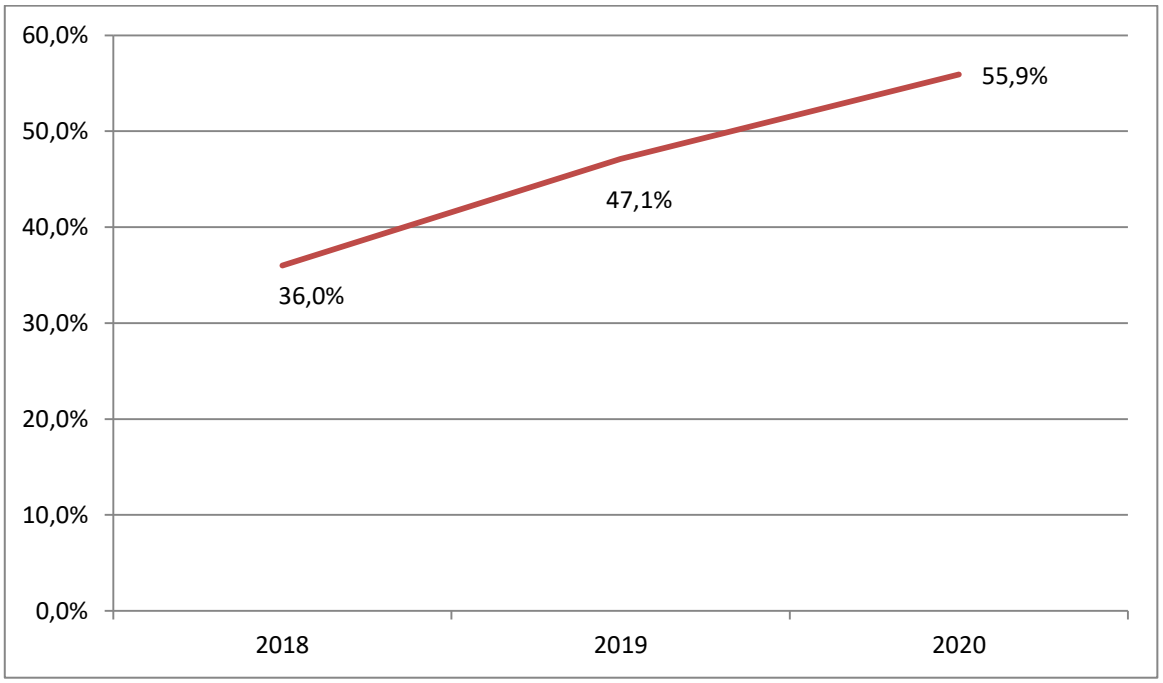


Рисунок 4. Рост доли утечек по вине внешних нарушителей, 2018 - 2020 гг.

На рисунке ниже приводится сравнение количества утечек по вине внутреннего и внешнего нарушителя (по вектору воздействия) за 2019 и 2020 год (Рисунок 5).

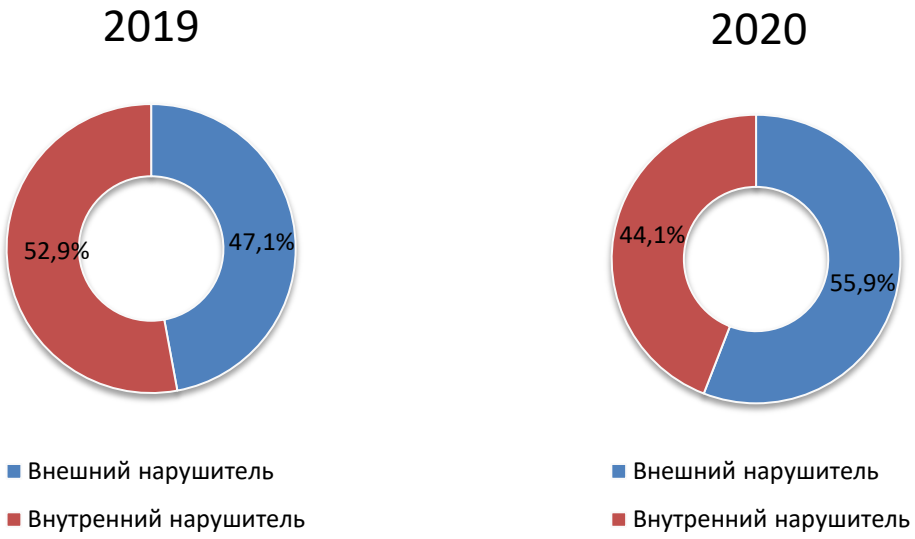


Рисунок 5. Распределение утечек по вектору воздействия, 2019-2020 гг.

На фоне пандемии и массового перехода на удаленную работу стало намного больше уязвимых точек для входа в корпоративные сети, чем не преминули воспользоваться хакеры.

Таким образом, количество утечек по вине внешнего нарушителя выросло с 47% в 2019 году до 56% в 2020 году.

Ситуацию усугубляют особенности законодательства англосаксонских стран, на которые приходится примерно половина всех зарегистрированных ЭАЦ утечек. Регуляторы этих стран строго предписывают сообщать об утечках, иначе компаниям грозят крупные штрафы и долгие судебные разбирательства. В такой ситуации жертвам утечек выгоднее списать вину на внешних злоумышленников («русских хакеров» или иных лиц), даже когда утечка произошла в результате действий персонала.

Далее рассмотрим, сколько записей ПДн и платежной информации в среднем утекало в результате одной утечки, вызванной внутренним и внешним нарушителем, и изменение соотношения подобных среднестатистических утечек за последние три года (Рисунок 7).

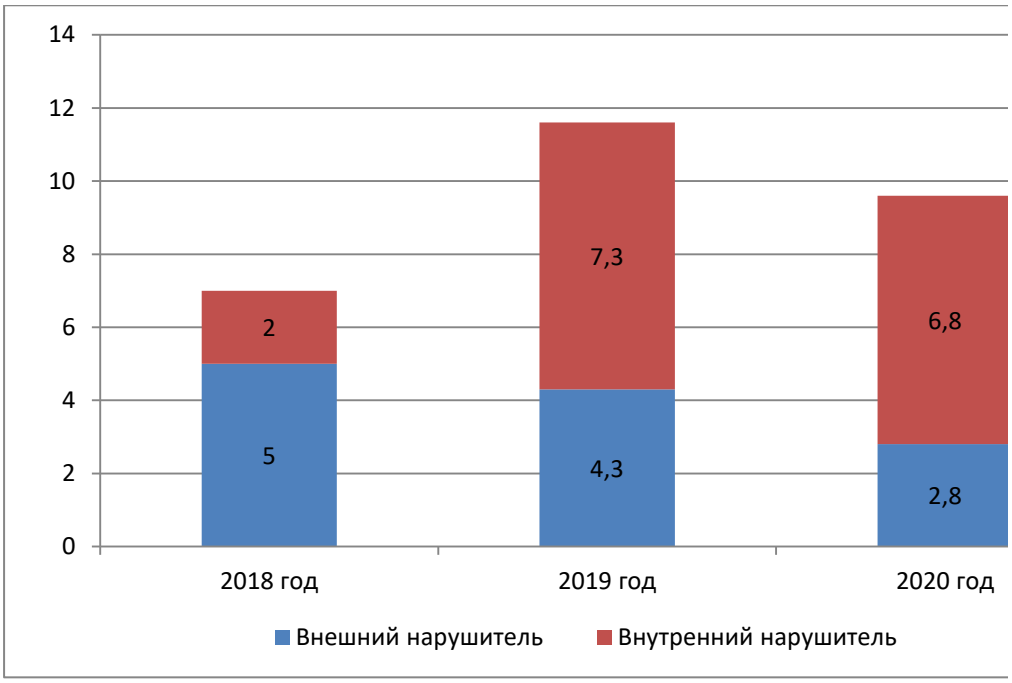


Рисунок 7. Среднее число скомпрометированных записей (в млн) в результате одной утечки, вызванной внутренними и внешними нарушителями, 2018-2020 гг.

> *InfoSecurity Magazine: Исследователи безопасности обнаружили незащищенную базу данных с личной информацией популярного приложения для тренировок Kinomap. В базе объемом 40 ГБ были записи 42 млн пользователей со всего мира, включая Северную Америку, Австралию, Японию, Великобританию и несколько стран Евросоюза. В скомпрометированной базе хранились полные имена, адреса электронной почты, страны проживания и метки времени для упражнений. Некоторые данные раскрыты опосредованно. Многие записи содержали ссылки на профили Kinomap со сведениями об их активностях. Исследователи утверждают, что также на сервере находились ключи доступа к API Kinomap, которые хакеры могут использовать для взлома учетных записей и блокировки их владельцев.*

В 2019-2020 годах значительно сократился объем данных, скомпрометированных в результате одной утечки, вызванной внешним воздействием. В среднем на одну «внешнюю» утечку в 2020 году пришлось 2,8 млн скомпрометированных записей. Вероятно, хакеры стали более разборчивы в своих предпочтениях и, проникнув в сеть компании, стараются украсть самую ликвидную информацию.

При этом в результате одной утечки данных по вине внутреннего нарушителя было скомпрометировано в среднем 6,8 млн. записей. Такое соотношение связано, в первую очередь, с бурным развитием облачных сервисов и накоплением в хранилищах огромных объемов информации, которая может утекать из-за халатности сотрудников. Речь идет прежде всего о некорректных настройках хранилищ в облачных сервисах типа Amazon и MongoDB, а также допущенных уязвимостях на веб-сервисах.

На рисунке ниже представлено соотношение общего объема записей, скомпрометированных в результате утечек по вине внешних и внутренних нарушителей за 2020 г.

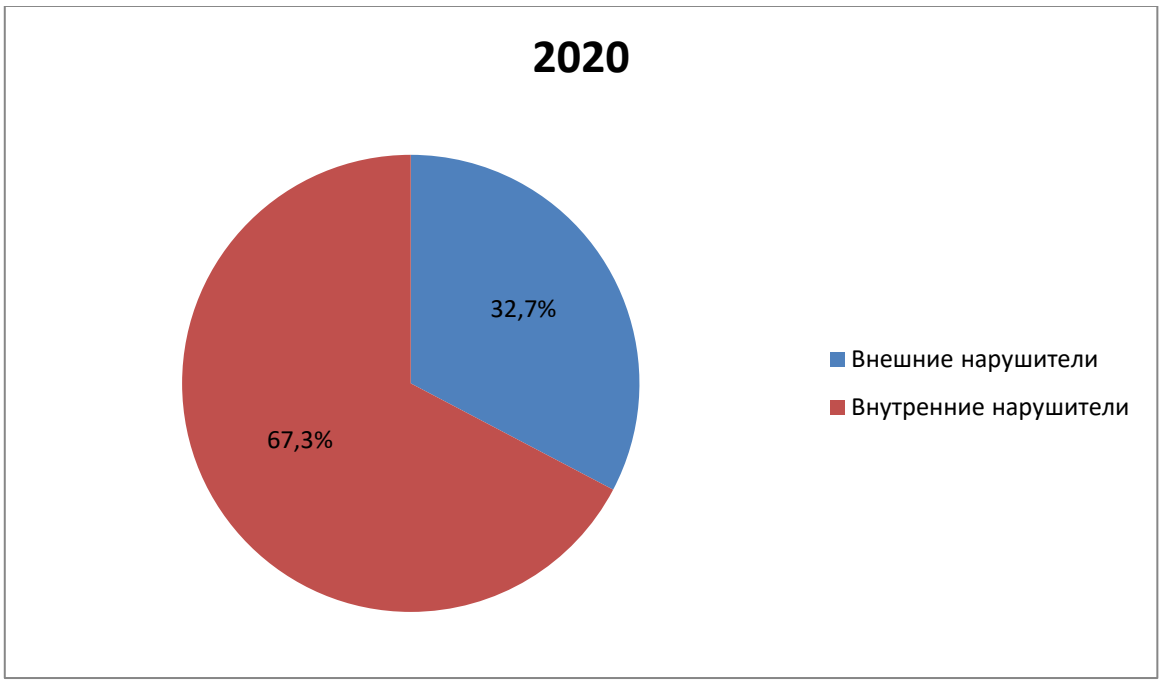


Рисунок 8. Доли общего объема записей, скомпрометированных в результате утечек по вине внешних и внутренних нарушителей, 2020 г. (%)

По вине внешнего нарушителя за 2020 год было скомпрометировано 3,57 млрд записей — это составляет 32,7% от совокупного объема скомпрометированных за год записей. Соответственно, на утечки, спровоцированные внутренним нарушителем, пришлось 7,33 млрд записей, что составляет 67,3% (Рисунок 8). ***То есть более 2/3 конфиденциальных данных утекало в результате как умышленных, так и случайных действий персонала компаний.*** Примерно такое же соотношение было зафиксировано по итогам 2019 года. Тогда на внешних нарушителей пришлось 32,4% скомпрометированных записей, а на внутренних - 67,6%.

Нельзя исключать того, что многие умышленные действия остались незамеченными вследствие отсутствия средств контроля работы основной массы удалённых сотрудников, а информация, похищенная ими, пока не поступила в открытую продажу.

44 «мега-утечки» из зарегистрированных в 2020 году относятся к типу внутренних, т.е. являются следствием неправомерных действий (бездействия) представителей категории «внутренний нарушитель».

К 36 утечкам, в результате каждой из которых утекло от 10 млн записей, привели хакерские атаки и другие действия внешних нарушителей.

Еще в четырех случаях «мега-утечек» объем опубликованной информации не позволил определить вектор утечки.

The Threat Post: Аналитики компании vpnMentor обнаружили в облаке несколько незащищенных баз данных, относящихся к религиозному приложению Pray.com. В кластерах сервиса Amazon исследователи насчитали более 1,9 млн различных файлов общим объемом 262 ГБ. Большая часть скомпрометированных данных представляли внутренние документы, однако один из кластеров содержал порядка 80 тыс. файлов с персональными данными подписчиков приложения. Число людей, которых затронула эта утечка, vpnMentor оценивает в 10 миллионов. В файлах были списки приходов, с подробной информацией о каждом прихожанине, включая имена, домашний и электронный адреса, номера телефонов и семейное положение. По словам исследователей, самое неприятное в этой утечке то, что были скомпрометированы телефонные справочники пользователей.

Business Insider: Исследователи безопасности обнаружили на черном рынке объявление о продаже данных порядка 20 млн клиентов индийской службы доставки продуктов BigBasket. База данных стартапа продается за $40 тыс. По данным Cyble, украденные в BigBasket данные могут включать имена пользователей, адреса электронной почты, хэшированные пароли, пин-коды, контактные номера, адреса, даты рождения, сведения о местоположении и IP-адреса.

Далее мы исследовали общую совокупность записей ПДн и платежной информации, скомпрометированных в результате действий (как умышленных, так и случайных) внутренних нарушителей Выяснилось, что 2020 году 98,2% записей среди утечек внутреннего характера утекли в результате случайных нарушений со стороны персонала. То есть всего 1,8% записей из совокупности внутренних утечек были украдены или разглашены.

Такая колоссальная доля записей, скомпрометированных непреднамеренно, не должна удивлять: утечки случайного характера приводят к компрометации больших, порой многомиллионных, баз данных – например, вследствие неправильных настроек облачных хранилищ или изъянов, допущенных в ходе разработки приложений и веб-сайтов. Внутренние нарушители далеко не всегда могут быстро, оставаясь незамеченными, скачать огромные объемы данных. Обычно такие нарушители нацеливаются на определенные фрагменты баз данных – записи, которые можно выгодно продать по заказу или использовать самостоятельно в мошеннических целях.

Хакерские атаки вышли на первый план

В 2020 году повышенная доля утечек внешнего вектора нашла отражение и в увеличении процента случаев компрометации данных по вине внешних нарушителей (хакеров) и неизвестных лиц. На эту категорию нарушителей пришлось 60,5% зарегистрированных утечек, тогда как годом ранее на них пришлось 52,5% случаев. Подробнее на рисунке 9.

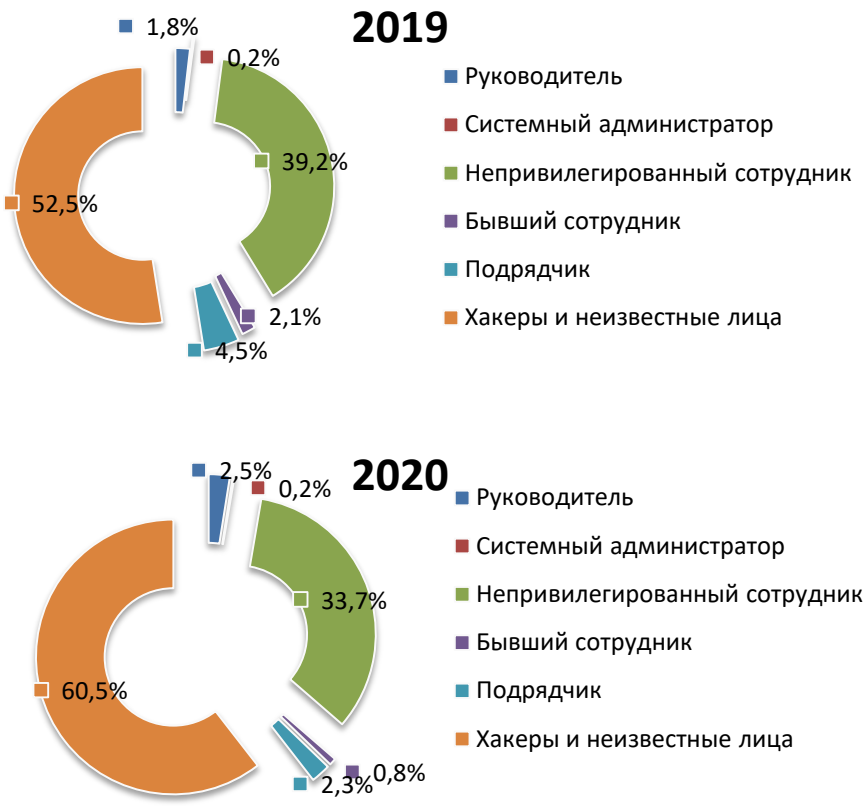


Рисунок 9. Распределение утечек по источнику (виновнику), 2019-2020 гг.

Что касается внутренних нарушителей, то доля утечек по вине непривилегированных сотрудников сократилась с 39,2% до 33,7%. При этом доля зарегистрированных случаев потери или кражи данных в результате действий привилегированных пользователей – руководителей разного уровня и системных администраторов – выросла с 2% до 2,7%. На долю подрядчиков и бывших сотрудников в сумме за 2020 год пришлось 3,1% утечек – вдвое меньше, чем в 2019 году. Вероятно, многие компании стали лучше контролировать потоки данных, которые проходят через партнеров, и в последнее время более внимательно подходят к управлению доступом, своевременно аннулируя учётные записи ушедших сотрудников или подрядчиков, работы которых завершены.

> *RTL Today: В руки журналистов попали документы органов правосудия одной из самых маленьких стран Европы. Представитель судебной администрации Люксембурга Анри Айперс (Henri Eippers) подтвердил, что похищены многочисленные документы (общим объемом около 1 ГБ) о судебных делах. Затем неизвестное лицо передало украденные файлы представителю прессы. Злоумышленники унесли конфиденциальные данные, включая отчеты, протоколы и данные электронной переписки. Кроме того, ряд документов содержат персональные данные граждан и конфиденциальные сведения об организациях. По словам Айперса, утечка, по-видимому, не произошла в результате атаки хакеров на серверы органов правосудия. Также практически исключен взлом Государственного ИТ-центра (CTIE). Предположительно, данные были скопированы на флэшку или вынесены из помещения на бумаге.*

Платежные данные все сложнее монетизировать, но более ликвидными на черном рынке становятся ПДн

В распределении зарегистрированных утечек по типам данных обращает на себя внимание снижение вдвое доли платежных данных (Рисунок 10).

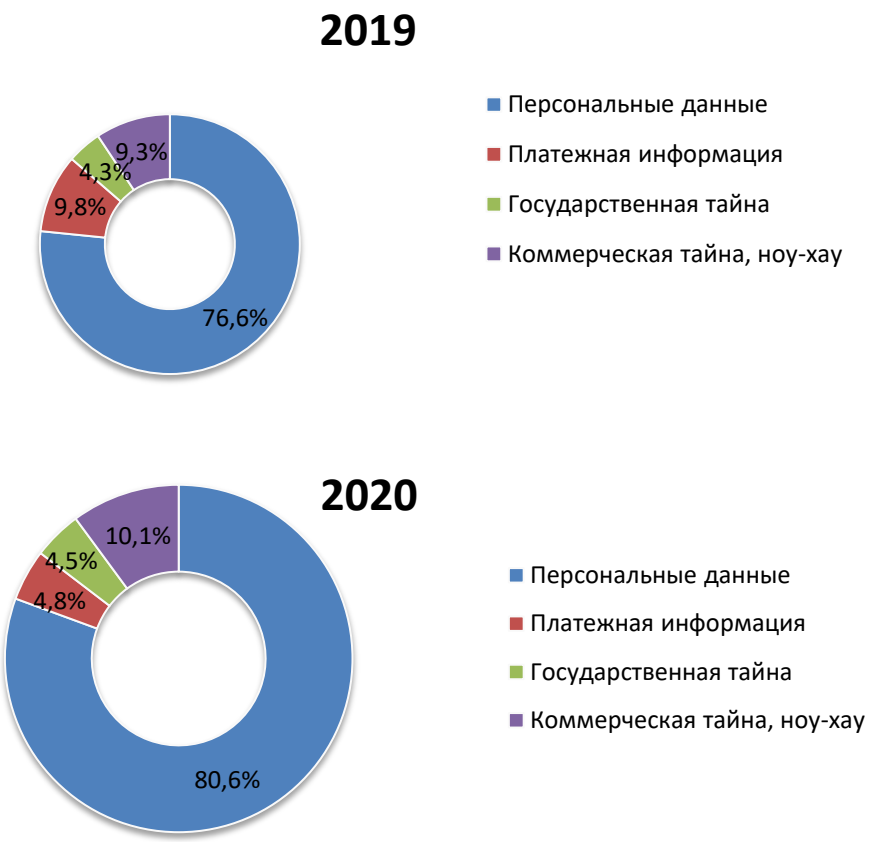


Рисунок 10. Распределение утечек по типам данных, 2019-2020 гг.

На наш взгляд, такое заметное изменение имеет объяснение.

Во-первых, компании из финансовой сферы усилили защиту платежной инфраструктуры и соответствующих систем хранения данных (мы писали об этом в отчёте, посвященном утечкам в 2020 году в финансовой сфере).

Во-вторых, украденные данные банковских карт в последнее время все труднее становится использовать для получения денежных средств: банки оперативно блокируют скомпрометированные карты как самостоятельно, так и по обращениям пользователей.

В-третьих, с увеличением количества цифровых сервисов, возможностей удаленной работы у злоумышленников стало больше способов монетизировать персональные данные: оформить кредит, получить налоговый вычет на основе информации того или иного человека, использовать записи ПДн для совершения фишинговых атак и т.д. Во второй половине 2020 года в России был принят ряд поправок к законам, которые должны затруднить жизнь подобным злоумышленникам.

Возможно, именно с этим связно общее снижение в мире доли прямых мошеннических действий с «утекшей» информацией (см. далее).[3]

Доля коммерческой тайны в распределении по типам данных выросла незначительно. Ровно в половине случаев различные корпоративные секреты и ноу-хау похищали хакеры и неустановленные лица, другую половину случаев составили утечки по вине различных категорий сотрудников. Подобная конфиденциальная информация – желанная цель для нарушителей, которые завербованы конкурентами, хотят обеспечить себе комфортные условия на новом месте работы или стремятся запустить собственные стартапы. Подробнее об этом читайте в главе, посвященной действиям увольняющихся сотрудников.

> *Bloomberg.com: Корпорация Mars подала в суд на сеть закусочных и кофеен Pret Panera, а также ее материнскую компанию JAB, обвиняя их в использовании тысяч конфиденциальных документов. Согласно исковому заявлению Mars, один из бывших топ-менеджеров корпорации Яцек Саржински (Jacek Szarzynski) передал структурам JAB множество секретных документов, включая финансовые прогнозы, данные о продажах товаров различными продуктовыми направлениями, а также сведения, касающиеся возможных сделок. В Mars выяснили, что Яцек Саржински неоднократно похищал внутренние документы в период ведения переговоров с JAB. Корпорация отмечает, что ее бывший топ-менеджер закачивал данные на служебный ноутбук, а затем копировал их на внешний жесткий диск. В дальнейшем Саржински неоднократно делился украденной информацией со своими новыми коллегами, считают истцы.*

Доля прямого мошенничества с «утекшими» данными сократилась

Довольно неожиданные итоги дало исследование распределения инцидентов по характеру. Подробнее на рисунке ниже.

[3] В целях данного исследования под прямыми мошенническими действиями мы пониманием мошенничество (попытку) использовать данные для получения денег или иной выгоды сразу после их получения, как правомерного (сотрудники кредитных организаций и т.п.), так и неправомерного.

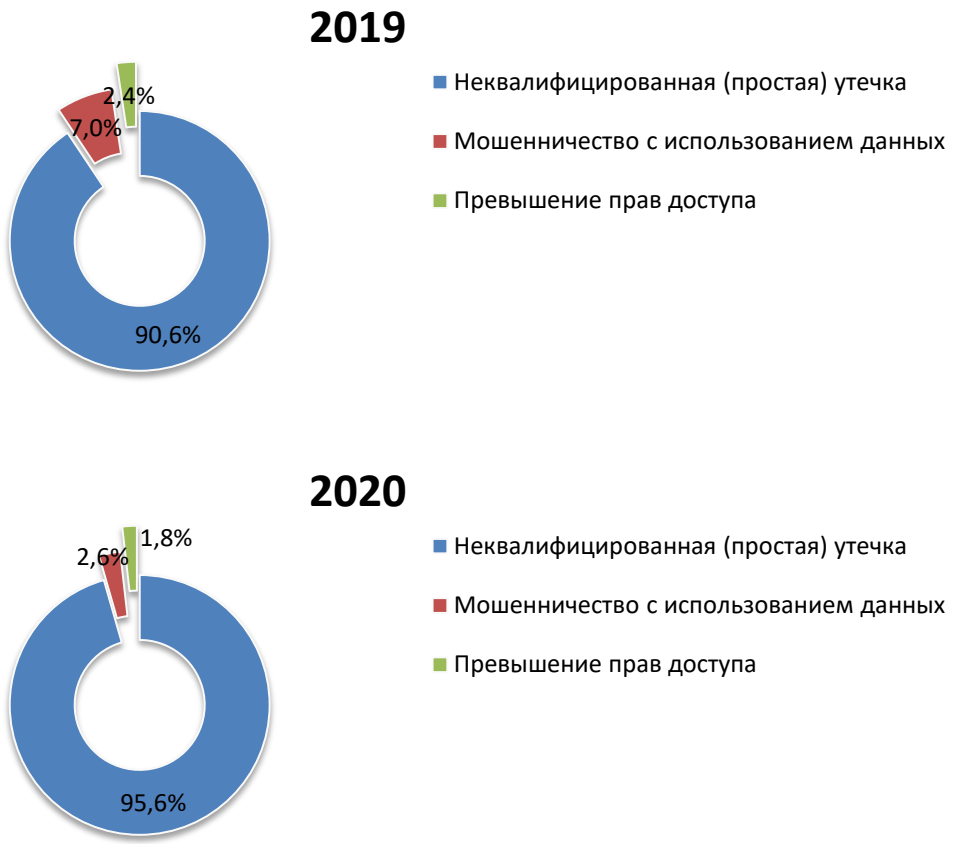


Рисунок 11. Распределение инцидентов по характеру, 2019-2020 гг.

Доля утечек, которые прямо не связаны со случаями мошенничества или нарушения прав доступа, в 2020 году выросла с 90,6% до 95,6% (Рисунок 11). На наш взгляд, это связано с тем, что многим похитителям информации стало неинтересно самим использовать ее в мошеннических целях, за исключением рядовых работников, попытавшихся «монетизировать» доверенные им персональные и платёжные данные. В подавляющем большинстве случаев преступники стараются как можно быстрее продать пакеты добытых данных. И только пройдя несколько «рук», украденная информация обычно становится «топливом» для разного рода махинаций. Украденная база может продаваться оптом или дробиться на фрагменты. Зачастую, исчерпав потенциал монетизации добытых данных, хакеры сливают базы в открытый доступ, после чего конфиденциальная информация становится доступна всем желающим.

Соответственно, доля утечек данных, сопряженных с последующим использованием скомпрометированной информации в целях мошенничества (как правило, речь идет о банковском фроде), снизилась с 7% до 2,6%. Однако пока с большой долей осторожности можно говорить о коренном переломе в борьбе с фродом, где речь идет о прямом использовании пользовательских данных нарушителями в мошеннических целях. Вероятно, многие мошеннические случаи во время пандемии остались незамеченными. При этом далеко не везде фрод отступает. Так, в России о непростом положении свидетельствуют данные ЦБ, согласно которым число денежных

операций, совершенных без согласия клиентов, в 2020 году выросло на 23,1%, возможно, что этому способствовал рост утечек ПДн.

К нарушениям, связанным с получением сотрудниками доступа к данным, которые не требуются для выполнения служебных обязанностей, в 2020 году ЭАЦ отнесены 1,8% инцидентов против 2,4% в 2019 году.

США: выявленных утечек стало существенно меньше

В распределении утечек по странам первую позицию в прошлом году вновь заняли Соединенные Штаты Америки (США), где было зарегистрировано 938 утечек (39,2% от общего объема утечек в мире). При этом годом ранее Штаты занимали долю 44,7%, а общее число утечек там было почти на 20% больше - 1123 случая. В 2018 г. утечек было 956. ***Таким образом, именно США в первую очередь повлияли на изменение общемировой картины с точки зрения количества выявленных утечек.*** Для США 2020 год был очень непростым не только в экономическом плане (тяжелые испытания для экономики, вызванные влиянием пандемии), но и в политическом (протесты движения BLM, штурм Капитолия, скандальные президентские выборы и т.д.). Многим компаниям в новых условиях было вдвойне сложно обеспечить требуемый уровень защиты конфиденциальной информации. Вероятно, немало случаев утечек могли быть скрыты, так как компании не хотели нести ответственность за инциденты в период турбулентности бизнеса.

Россия опять оказалась на втором месте — 404 утечки за 2020 год (395 в 2019 году, 270 в 2018 году).

На третьей строчке также без изменений – здесь располагается Соединенное Королевство Великобритании и Северной Ирландии со 143 случаями кражи и потери информации ограниченного доступа в 2020 году (121 случай в 2019 году, 124 – в 2018 году).

Каналы утечек

Рассмотрим далее долю утечек через сетевой канал от общего объема утечек (Рисунок 12).

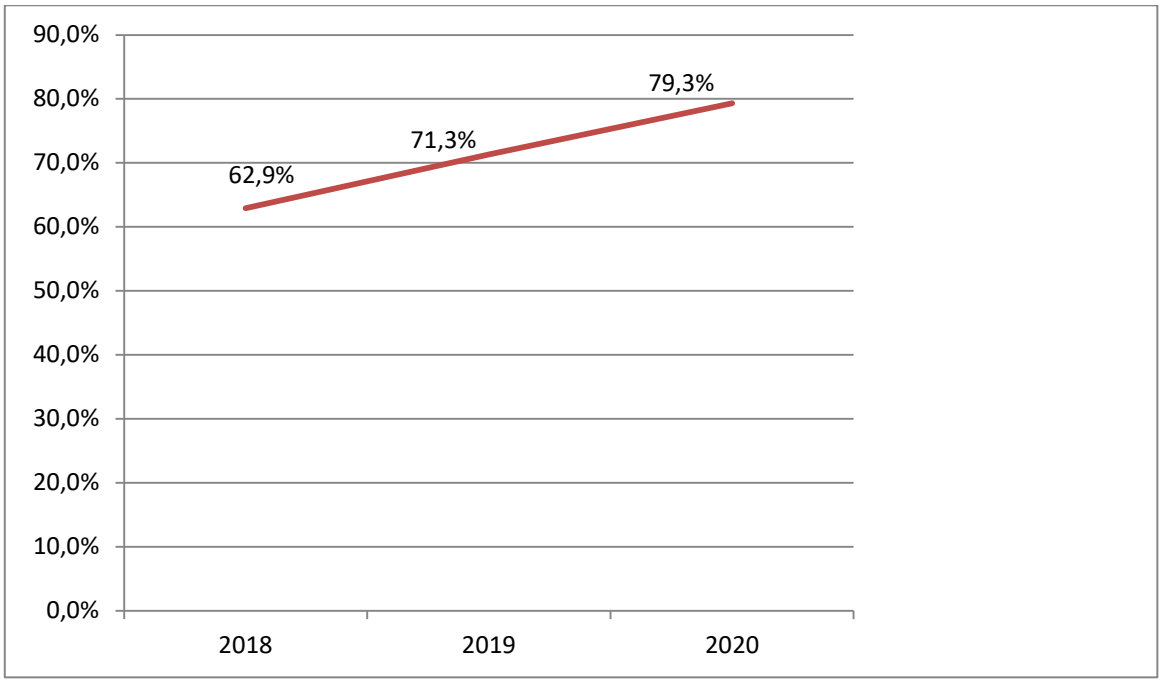
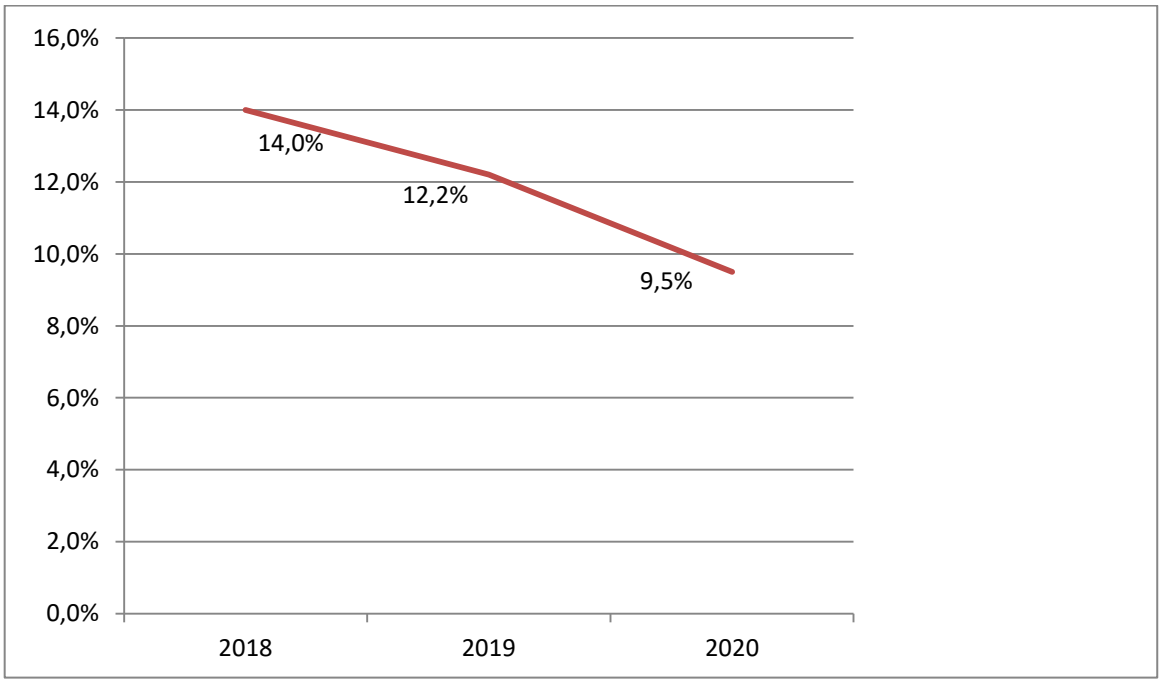


Рисунок 12. Доля Сети в распределении утечек по каналам, 2018-2020 гг.

Заметна тенденция к росту доли утечек, случившихся через Сеть[4]: согласно последним данным ЭАЦ, доля утечек через сетевой канал в 2020 году составила более 79,3%. В 2018 году данный показатель составил 62,9%.

Доля утечек по электронной почте, напротив, падает, согласно уточненным данным ЭАЦ (Рисунок 13). Этот канал активно используется для фишинговых атак, но, судя по всему, стал лучше контролироваться корпоративными службами безопасности, в том числе при массовом переходе сотрудников на дистанционный режим работы.



[4] См. Глоссарий

Рисунок 13. Доля электронной почты в распределении утечек по каналам, 2018-2020 гг.

Вместе с тем падает доля утечек через бумажные документы – в эпоху цифровизации этот канал становится все менее заметным, хотя говорить о его исчезновении в обозримом будущем вряд ли придется (падение почти в три раза по сравнению с 2018 годом, см. Рисунок 14).

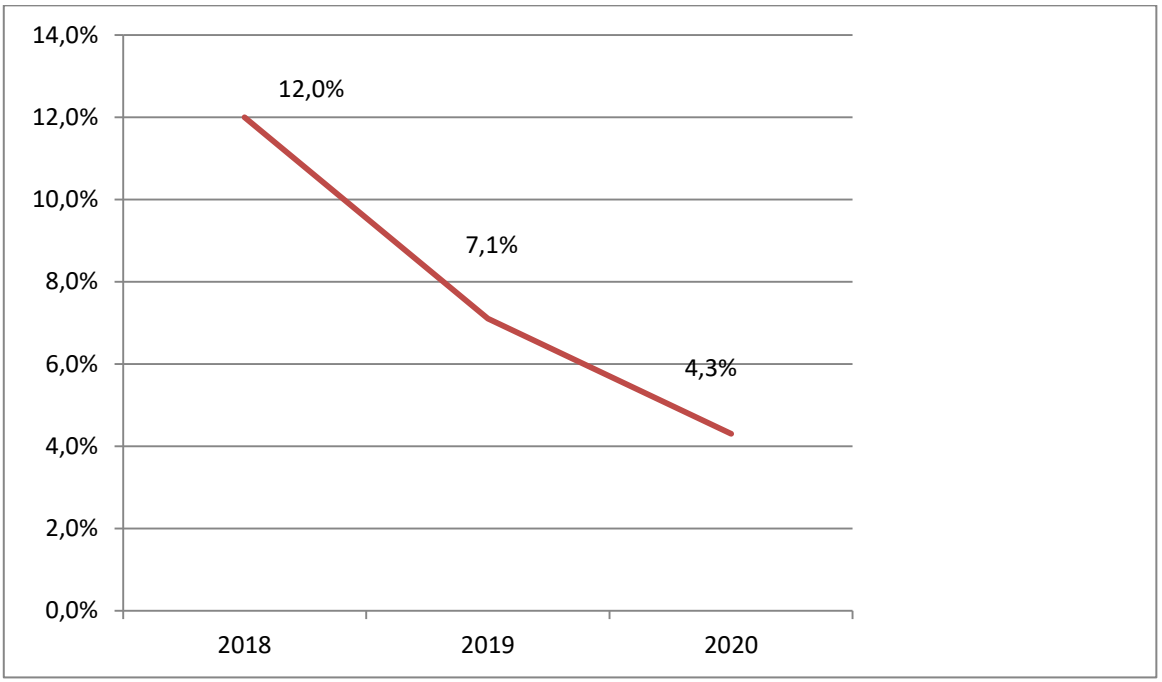


Рисунок 14. Доля бумажных документов в распределении утечек по каналам, 2018-2020 гг.

Также в 2020 году упала доля утечек в результате кражи или потери оборудования. При этом в среднем в мире практически не меняется доля утечек через каналы мгновенных сообщений, - остаётся в пределах 4-5% (Рисунок 15), хотя в России она составила без малого 20% – у нас мессенджеры становятся излюбленным средством передачи конфиденциальных данных недобросовестными сотрудниками.

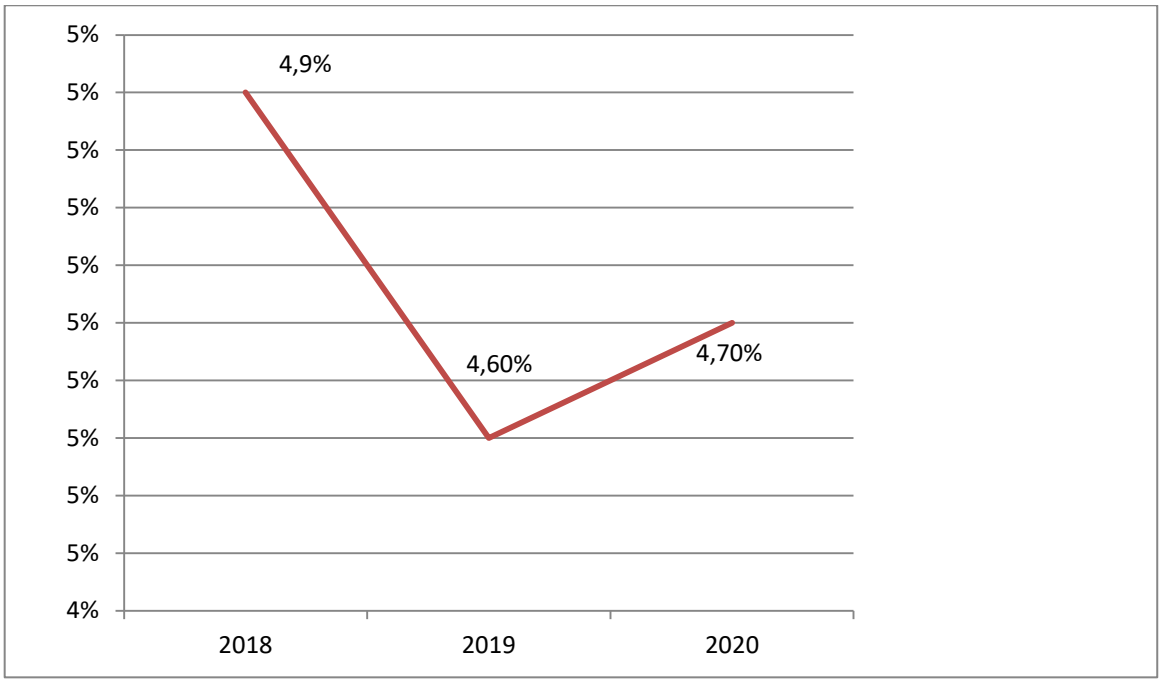


Рисунок 15. Доля мгновенных сообщений (мессенджеры) в распределении утечек по каналам, 2018-2020 гг.

Полное распределение утечек по каналам представлено на Рисунке 16.

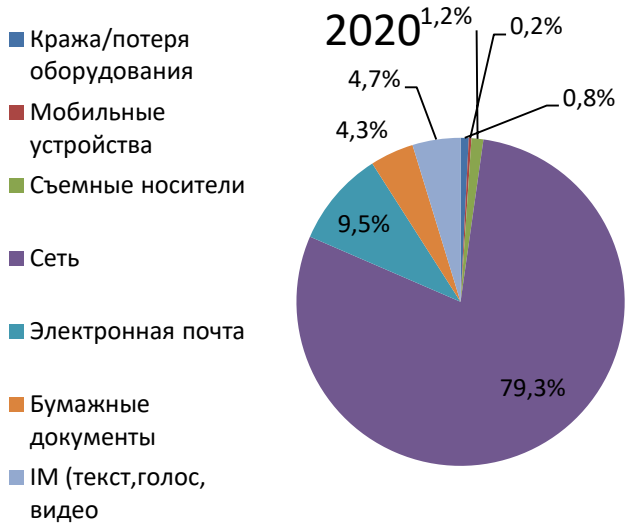


Рисунок 16. Распределение утечек по каналам, 2020 г.

В распределении по каналам не учтены неизвестные (неопределенные) случаи – традиционно таких утечек много, так как далеко не всегда авторы сообщений об утечках располагают информацией о том, каким путем были скомпрометированы утекшие данные. Авторы исследования при этом считают, что игнорировать наличие большого числа случаев с неопределенным каналом утечки методологически неправильно, поэтому решили отразить их на отдельной диаграмме.

На Рисунке 17 представлено распределение утечек по каналам с учетом доли неизвестных (неопределенных) случаев.

В 2020 году на неопределенные случаи утечек в распределении по каналам пришлось 8,2% случаев.

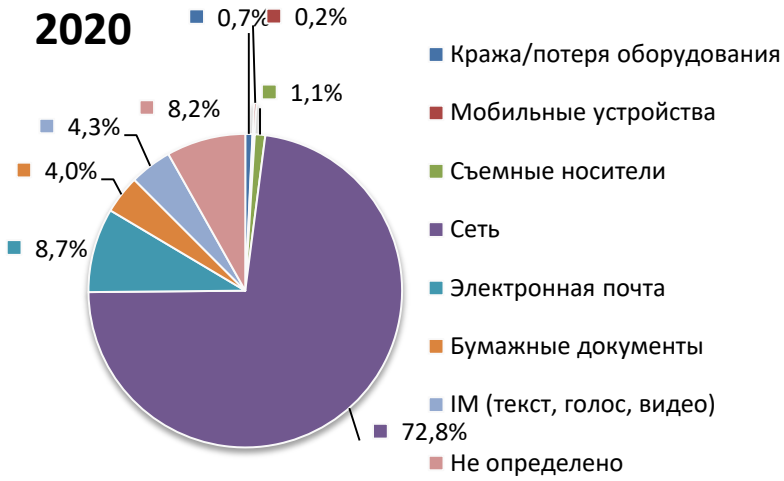


Рисунок 17. Распределение утечек по каналам с учетом доли неопределенных случаев, 2020 г.

В распределении утечек конфиденциальных данных в результате случайных, неумышленных действий заметен крен в сторону сетевого канала. В 2020 году доля Сети выросла до 73,1%. Роль электронной почты почти не изменилась, доли большинства других каналов стали менее заметными.

Распределение умышленных утечек также демонстрирует повышение роли Сети. Доля этого канала выросла с 75,2% до 81,6%. При этом стало меньше умышленных утечек по электронной почте, но больше через каналы мгновенных сообщений – IM (Рисунок 18).

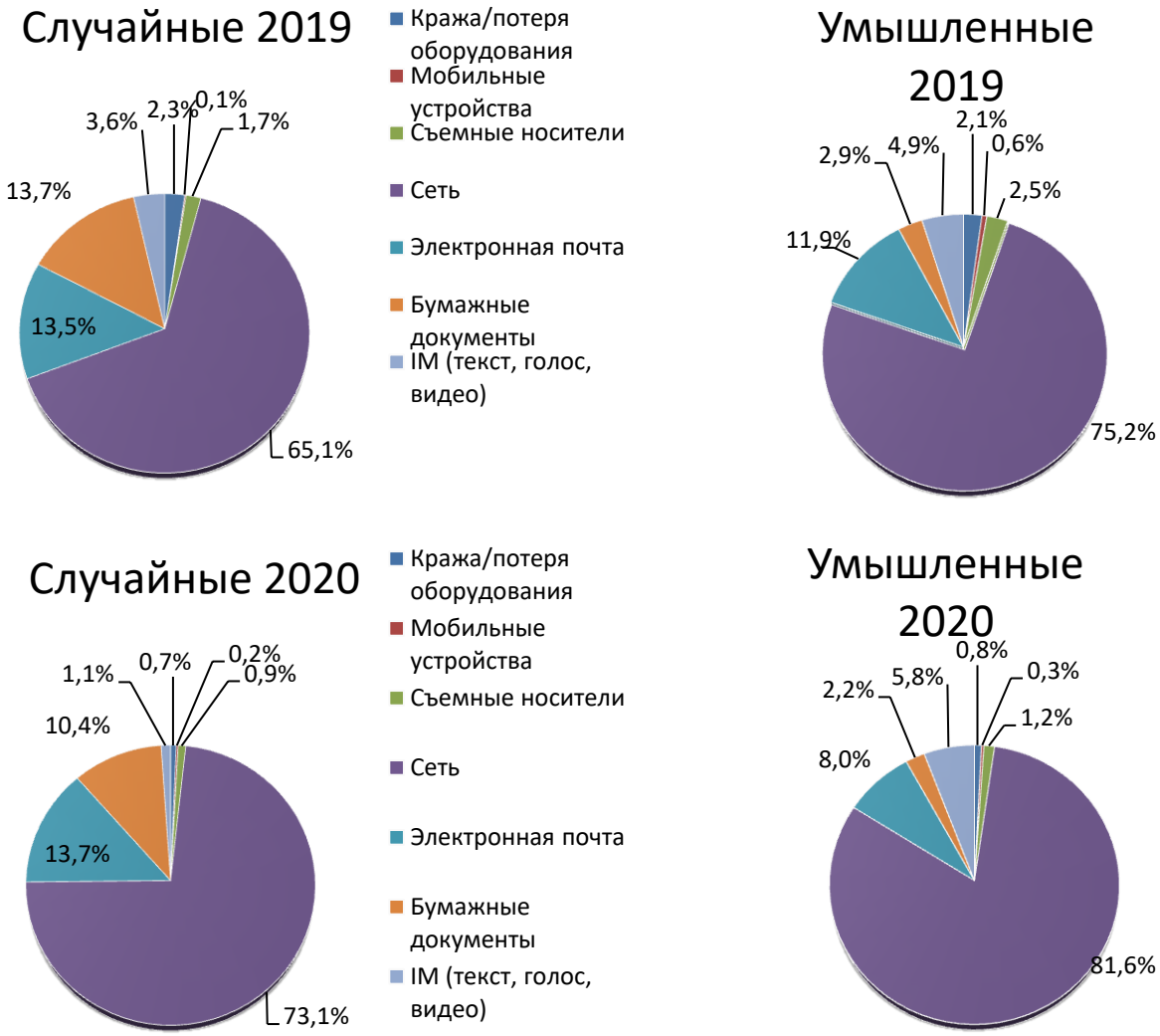


Рисунок 18. Распределение случайных и умышленных утечек по каналам, 2019-2020 гг. (%)

Распределение по отраслям

В распределении по отраслям существенных изменений в 2020 году не произошло. Наибольшая доля зарегистрированных утечек по-прежнему приходится на высокотехнологичные компании – в прошлом году она выросла до 19,5%. На втором и третьем месте вновь находятся медицинская сфера и госсектор, но доли утечек здесь упали (Рисунок 19).

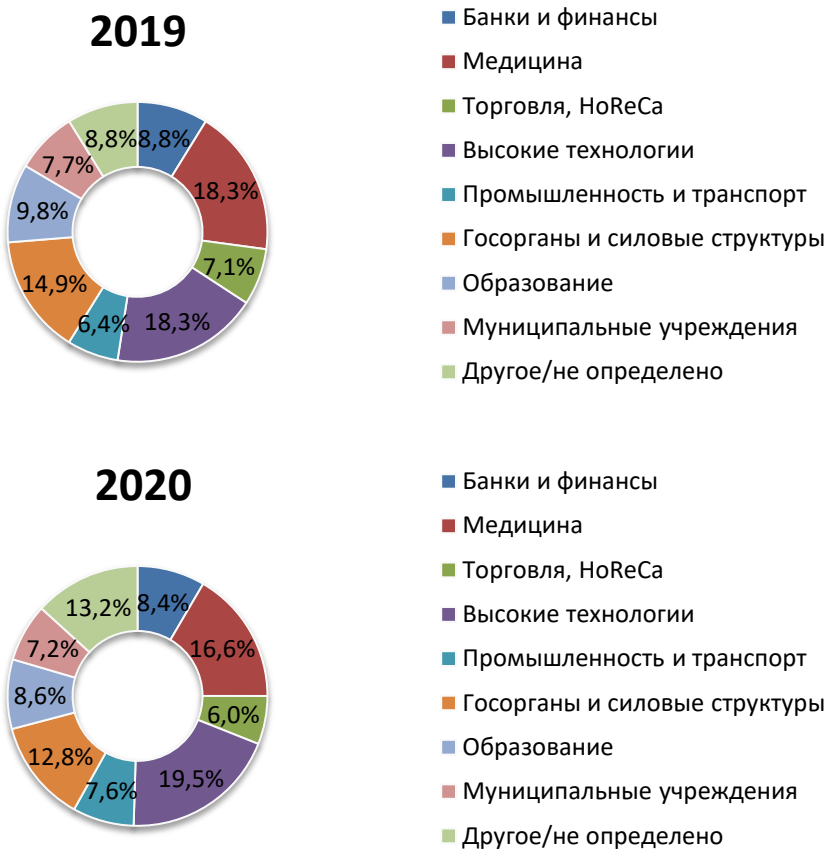


Рисунок 19. Распределение числа утечек по отраслям, 2019-2020 гг.

В рамках исследования мы определяем, какие отрасли привлекают нарушителей. Понятие «привлекательность» в данном контексте напрямую зависит от ликвидности данных, которые обрабатывают компании того или иного сегмента. То есть чем проще конвертировать украденную информацию в деньги («монетизировать»), тем отрасль выглядит привлекательнее для нарушителей.

Для составления сравнительной гистограммы авторы используют персональные данные как универсальный тип данных, общий для всех отраслей объект защиты, чтобы наглядно показать отраслевое распределение по «привлекательности».

Показателем привлекательности можно считать число умышленных утечек в конкретной отрасли. Для графической иллюстрации предлагается такое соотношение:

$$\text{Доля умышленных утечек} \leftarrow \frac{\text{Ликвидность данных}}{\text{Представление об уровне защищенности информации}}$$

В 2020 году наиболее привлекательными для нарушителей оказались сферы финансов и образования. В них более 80% зарегистрированных утечек оказались умышленного характера (Рисунок 20).

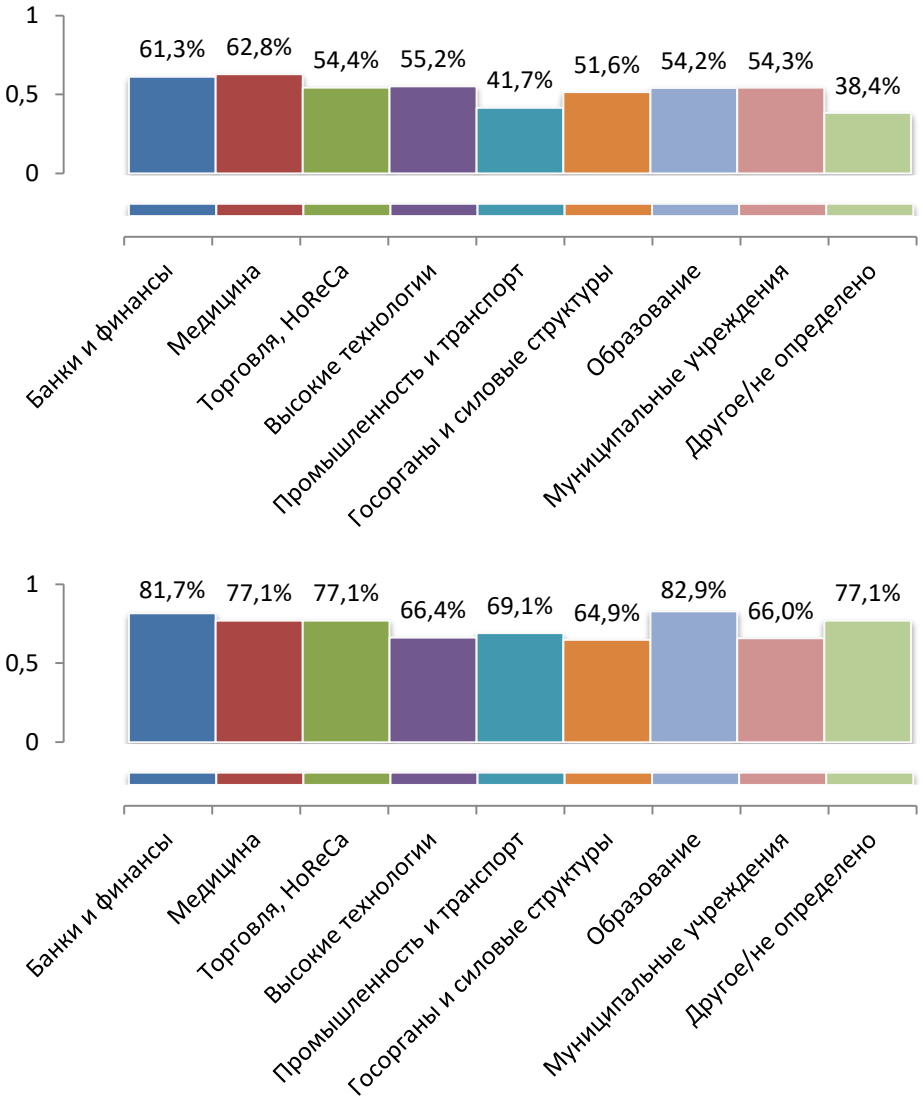


Рисунок 20. Доля умышленных утечек ПДн от общего количества утечек ПДн по отраслям, 2019-2020 гг.

В целом, всплеск доли умышленных утечек отмечен во всех отраслях, что в первую очередь связано с существенным ростом ликвидности данных в период пандемии: в это время недобросовестные сотрудники активно искали дополнительный заработок, а хакеры пользовались тем, что компании в авральном режиме меняли привычные формы реализации процессов и могли при этом ослабить контроль информационных активов. В результате совокупная доля умышленных утечек составила 72,5%, тогда как годом ранее было 60,2%.

Исследование инцидентов ИБ, связанных с действиями увольняющихся сотрудников

Увольняющиеся сотрудники – категория, требующего особого внимания корпоративных служб безопасности. Даже самый лояльный сотрудник, приняв решение об увольнении, может резко поменять модель поведения и использовать (попытаться использовать) информационные ресурсы работодателя в личных целях.

Риск кражи информации повышается в ситуациях, связанных с переманиванием сотрудника конкурентами или его желанием открыть собственный бизнес. Сотрудник также может руководствоваться мотивами мести или выступать «пешкой» в руках умелых манипуляторов, в том числе играющих на любовных чувствах.

Специалистам служб безопасности можно и нужно управлять рисками, связанными с увольнением сотрудников. Путем анализа внутренних потоков с помощью специальных решений по предиктивной аналитике, можно с высокой степенью точности предсказать увольнение сотрудника по собственному желанию задолго (порой даже за полгода) до подачи заявления.

В число основных деструктивных действий со стороны увольняющихся сотрудников в отношении информационных активов организации входят неправомерное модифицирование, уничтожение, копирование, предоставление и распространение информации. В большинстве случаев увольняющийся нарушитель копирует конфиденциальные данные и передает (продаёт) их третьим лицам или использует для создания собственного бизнеса. Ситуации с распространением чаще встречаются в случае мести. На рисунке 21 представлено распределение утечек, связанных с действиями увольняющихся сотрудников, по объектам воздействия, то есть источникам хранения конфиденциальной информации.

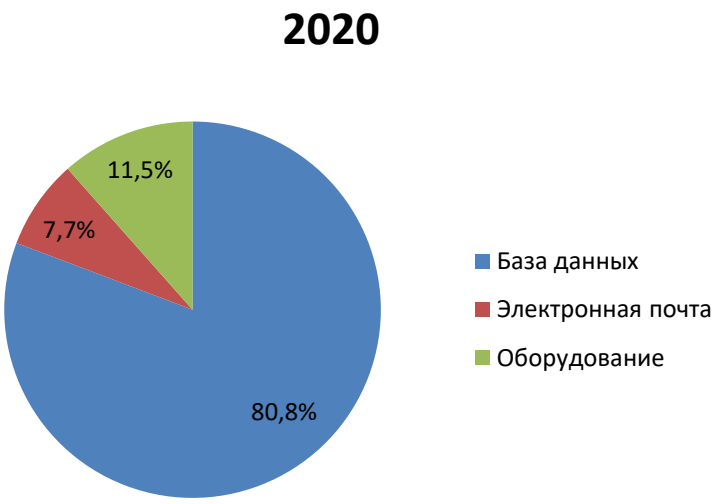


Рисунок 21. Источники конфиденциальной информации: объект воздействия увольняющегося нарушителя, 2020 г.

Bloomberg Law: Компания Hershey, крупнейший производитель кондитерских изделий в США, подала в суд на бывшего президента подразделения диетических снэков Amplify Дага Беренса (Doug Behrens). Согласно судебным документам, в Hershey установили, что в период между подачей заявления об увольнении и последним днем работы в компании Даг Беренс отправил на личный адрес электронной почты порядка 100 конфиденциальных документов. Среди них было несколько презентаций, посвященных стратегии компании, список клиентов Amplify и особенности их потребительских предпочтений, а также схематическое представление VIP-клиентов подразделения. В исковом

заявлении Hersheys подчеркивается, что компания в полной мере не знает о деяниях Дага Беренса, так как он перед увольнением удалил все данные со своего корпоративного ноутбука.

В 80% изученных случаев, зарегистрированных в 2020 году, нарушители из числа увольняющихся сотрудников обращались к различным базам данных работодателя, в 11,5% случаев уносили рабочее оборудование, на котором хранились данные. Как правило, речь идет о том, что после увольнения сотрудники забирали с собой корпоративные ноутбуки, где хранилась информация, накопленная за время работы в компании. Еще в 7,7% случаев увольняющиеся нарушители пересылали на сторонние адреса электронной почты письма из корпоративной переписки, файлы, где были записи с коммерческой информацией и другими конфиденциальными сведениями.

Как правило, увольняющиеся сотрудники стараются унести из компании информацию, относящуюся к коммерческим секретам и ноу-хау, то есть те данные, с помощью которых можно запустить собственный бизнес, выгодно продать их конкурентам или создать комфортную стартовую площадку у нового работодателя (Рисунок 22). Отметим, что в ряде случаев статус коммерческой тайны могут иметь и клиентские базы, одновременно являющиеся ИСПДн.

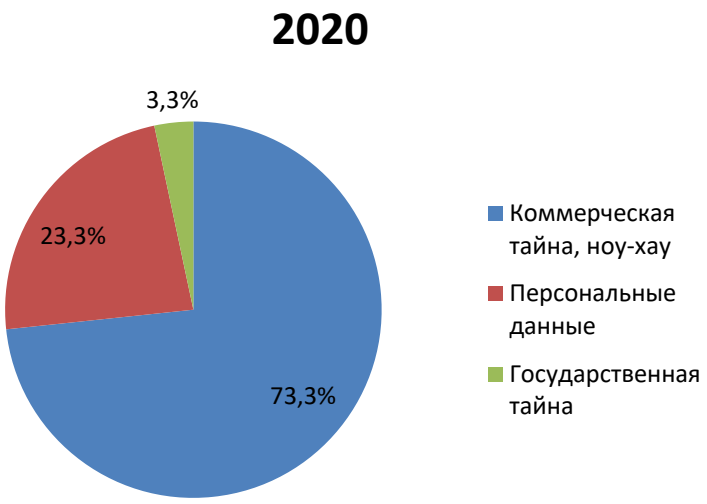


Рисунок 22. Типы конфиденциальной информации, скомпрометированной увольняющимися нарушителями, 2020 г.

The Real Deal: Компания Bespoke Real Estate подала в окружной суд Нью-Йорка на бывшего сотрудника Престона Кея (Preston Kaye). Мужчину обвиняют в краже конфиденциальной информации о рынке недвижимости В Bespoke утверждают, что Кей регулярно отправлял корпоративные документы на свою личную электронную почту и аккаунт iCloud. Судя по всему, перед увольнением сотрудник копировал документы со сведениями о потенциальных покупателях и продавцах элитной недвижимости.

Почти 2/3 нарушений, допущенных увольняющимися сотрудниками в отношении информационных активов работодателя, связаны со стремлением передать конфиденциальные данные сторонним компаниям, прежде всего конкурентам (Рисунок 23).

Рисунок 23. Основные мотивы увольняющихся нарушителей, 2020 г.

Примерно 1/3 нарушителей относятся к числу привилегированных сотрудников - руководители и системные администраторы (Рисунок 24).

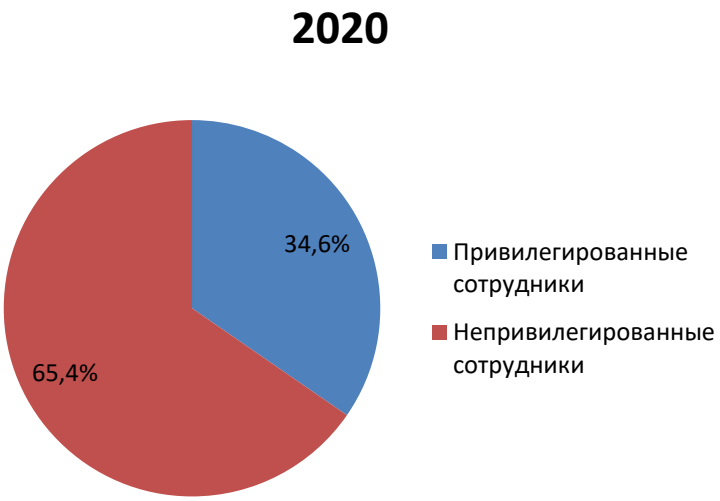


Рисунок 24. Категории увольняющихся нарушителей, 2020 г.

PharmaLive: Американская компания Abbott, производитель медицинского диагностического оборудования и лекарственных препаратов, подала в суд на бывшего вице-президента Джерома Клавеля (Jerom Clavel), обвиняя его в похищении конфиденциальной информации и передаче ее новому работодателю. Согласно исковому заявлению Abbott, в тот день, когда Клавель покинул свой пост якобы «по состоянию здоровья», он принял предложение

калифорнийской диагностической компании Bio-Rad Laboratories, где в итоге занял должность вице-президента по маркетингу подразделения клинической диагностики. Вскоре после ухода Клавеля в компании обнаружили, что бывший руководитель загружал на внешние устройства хранения документы с корпоративного ноутбука. Также утверждается, что Клавель отправлял на личный адрес электронной почты рабочую переписку, где, в частности, была конфиденциальная информация о прогнозах роста бизнеса на развивающихся рынках, а также сведения о продуктах Abbott для проведения тестов на коронавирусную инфекцию.

Чаще всего решившие покинуть компанию сотрудники начинают совершать неправомерные действия по отношению к информационным активам за несколько недель или даже месяцев до увольнения (Рисунок 25).

Примерно в четверти найденных сообщений об утечках по вине увольняющихся сотрудников не было информации о временном горизонте действий.

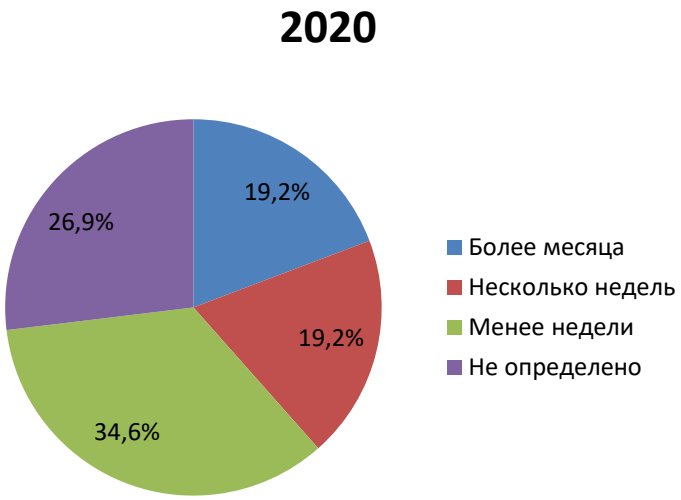


Рисунок 25. Совершение увольняющимися сотрудниками действий, повлекших ущерб. Время до увольнения, 2020 г.

Заключение

Почти весь 2020 год прошел под давлением пандемии коронавируса, что не могло не отразиться на развитии направления защиты информации. Массовый переход на удаленную работу и изменение многих привычных форм деятельности, бизнес-процессов, и, прежде всего, технологических процессов обработки информации привели к более уязвимому положению информационных активов, чем раньше.

На основании анализа данных из открытых источников может сложиться впечатление, что произошло снижение количества и общего объёма утечек по сравнению с 2019 годом, даже несмотря на ослабление контроля за обращением данных, вызванного массовым переходом на удалённую работу вследствие пандемии COVID-19.

Но проанализировав ситуацию за 3 последних года, мы видим, что продолжается рост количества умышленных утечек, доли утечек персональных данных и коммерческой тайны, увеличение доли сетевого канала одновременно со снижением роли бумажных документов и электронной почты.

Судя по всему, многие организации научились блокировать случайную передачу конфиденциальных данных – таких инцидентов фиксируется все меньше. Вместе с тем, большую опасность представляет рост доли утечек умышленного характера, вызванных как хакерскими атаками, так и действиями внутренних нарушителей. То есть, несмотря на то, что утечек внутреннего характера зарегистрировано существенно меньше, резкий рост умышленных нарушений среди них может говорить о недостаточном контроле за информационными ресурсами в компаниях на фоне значительного повышения ликвидности информации на черном рынке.

Несмотря на снижение количества зарегистрированных утечек и скомпрометированных записей ПДн и платежных данных, на наш взгляд, не приходится говорить о том, что 2020 год стал необычным и произошёл перелом в борьбе с утечками. Скорее, это 2019 год оказался аномальным на два количественных показателя за счёт «мега-утечек» (стало меньше составных баз) и роста латентности инцидентов. Возможно, в течение 2021 года мы получим больше информации об утечках, случившихся в 2020-м.

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. В базу попадают публичные сообщения[5] о случаях утечек информации из учреждений, организаций, предприятий любых организационных форм и форм собственности, включая органы государственной власти и управления.

В настоящий момент количество записей в базе превышает 20 000.

Исследования ЭАЦ в основном ориентированы на анализ сообщений об утечках данных на английском и русском языках, также используется некоторое количество источников на арабском, японском, немецком, французском, испанском и итальянском языках. Во многом с этим связана большая доля информации о российских утечках, сообщений об утечках из компаний англосаксонских стран и Европы. В целях данного исследования использовались публикации только на русском языке.

В ходе наполнения базы утечек ЭАЦ каждое сообщение об утечке классифицируется по закрытому списку признаков. Каждый признак обладает ограниченной вариативностью. К примеру, при классификации по страновой принадлежности, где каждому сообщению ставится в соответствие один из вариантов (название страны, на территории которой работает обладатель информации и где, предположительно, произошла утечка информации).

В базу вносятся:

- текст заголовка и сообщения об утечке,

[5] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках по всему миру.

- ссылка на источник сообщения,
- дата публикации сообщения,
- название предприятия (организацит, учреждения);
- государство (страна),
- сфера деятельности обладателя информации (отрасль),
- направление деятельности (коммерческая, некоммерческая),
- примерный размер пострадавшей от утечки организации (малая, средняя, крупная)[6],
- размер причиненного в результате утечки ущерба[7],
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- субъект[8], непосредственно допустивший утечку.

Выделяются следующие сферы деятельности (отрасли, отраслевые группы):

- банки, финансовые и страховые компании,
- медицина,
- торговля и HoReCa,
- высокие технологии (в основном ИТ и телекоммуникационные компании),
- промышленность, энергетика и транспорт,
- госорганы и силовые структуры,
- образование,
- муниципальные органы власти и учреждения,
- другое (некоммерческие организации, спорт, медиа, консалтинг, недвижимость и т.д.).

Далее каждое сообщение классифицируется по:

- наличию умысла[9] (если по описанию или имеющимся признакам действия лица, допустившего утечку, являются умышленными, то утечка классифицируется как умышленная; в обратном случае как неумышленная / случайная);
- каналу утечки,
- типам данных (относятся ли скомпрометированные сведения к персональным данным, платежной информации, государственной или коммерческой тайне, ноу-хау и т.п.),

[6] По предполагаемому количеству персональных компьютеров в компании. Малые – до 50 ПК, средние – от 50 до 500 ПК, крупные – более 500 ПК.

[7] Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ, или на сайтах пострадавших организаций, или из отчётов органов государственной власти, экспертных организаций.

[8] Авторы классифицируют утечки по виновнику инцидента. См. Глоссарий.

[9] Утечки данных разделяются на умышленные и неумышленные (случайные) См. Глоссарий.

- вектору воздействия (внешний, внутренний, не определено, в ряде случаев выделяем так называемый «гибридный вектор», когда утечка связана с влиянием как внешних, так и внутренних нарушителей),
- типу нарушителя.

Все перечисленные признаки (конкретные варианты признаков) вносятся при наличии информации, определяются методом экспертной оценки, носят вероятностный характер, если информация неполная или противоречивая. При невозможности классифицировать сообщение (нельзя выявить вариант признака и отразить в базе, если в сообщении об утечке прямо или косвенно нет указания признака), в соответствующем поле проставляется значение «неизвестно». Иных признаков (категорий для классификации) база утечек ЭАЦ не содержит.

Также в базу попадают случаи, когда невозможно установить обладателя скомпрометированной информации, но совершенно точно известно, что утекшая информация не является скомпилированным набором данных на основе других утечек. Такие случаи при добавлении в базу классифицируются по всем известным параметрам, а в поле отраслевой принадлежности ставится «другое», поле «название компании» остается пустым.

В базу вносится только количество записей, содержащих ПДн и/или платёжную информацию, т.к. в остальных случаях количественные характеристики обычно отсутствуют.

Важно отметить, что наряду с неквалифицированными «простыми» утечками авторы исследования выделяют «квалифицированные» утечки — случаи, когда деструктивное поведение сотрудников выражается в использовании легитимного (правомерного, санкционированного) доступа к данным в мошеннических целях (манипуляции с платежными данными, инсайдерской информацией); случаи превышения прав доступа, когда сотрудник знакомится, копирует, передает данные, к которым не должен иметь доступа по роду службы или работы. Указанные признаки также устанавливаются на основе экспертной оценки.

В случаях, когда тип нарушителя неизвестен, и удельный вес таких неизвестных в выборке незначителен (как правило, менее 3%), авторы исследования также добавляют их к внешним нарушителям, т.к. подобная выборка соответствует данным, полученным при изучении аналогичных случаев.

Сообщения об утечках (единицы совокупности или элементы выборки) в базе ЭАЦ далее именуются утечками. Т.е. каждая запись в базе ЭАЦ содержит сведения об одном событии, которое полностью соответствует приведенному выше определению утечки данных (информации).

Авторы считают, что большие шансы стать известными имеют случаи утечки данных, ставшие следствием:

- кражи в целях продажи неопределенному кругу лиц;
- действий хактивистов для достижения общественных и политических целей;

а также утечки из наиболее крупных и широко известных компаний, организаций, учреждений.

Кроме того, крупные утечки (объемом более 1 млн записей) и утечки из компаний с известными брендами чаще попадают в сферу внимания СМИ, блогеров, надзорных органов. Для анализа и корректного расчета среднего числа записей в одной публичной утечке выделена отдельная категория - «мега-утечка», то есть утечка, в результате которой было скомпрометировано 10 млн и более записей. Отдельно могут исследоваться и все утечки с числом скомпрометированных записей от 1 млн, а также вся совокупность утечек с числом записей до 1 млн.

Сведения об утечках представлены с использованием исторических данных — количественных показателей предыдущих лет.

Для повышения качества выводов использованы следующие подходы: исследования проводятся ежегодно на основе выборки, сформированной по единой методике (случайный поиск исходных сообщений об утечках, классификация сообщений по единому списку признаков). При формировании выводов авторы опираются на динамические показатели. Все данные в сравнительных исследованиях (сравнения с аналогичными показателями предыдущего периода) представляются в процентном виде. Исключение: сведения о совокупном количестве утечек, включенных в базу ЭАЦ, объеме записей, скомпрометированных в результате этих утечек, объеме скомпрометированных записей в расчете на одну утечку (только ПДн и платежная информация).

Указанные данные носят иллюстративный характер, дают представление, например, об изменении объемов определенных типов данных, хранимых и обрабатываемых обладателями информации.

В абсолютных показателях также представлены данные в виде так называемой «отраслевой карты утечек» — карта показывает фактическое распределение объема скомпрометированных персональных данных по отраслям (наглядно показывает зависимость объема ПДн в отрасли от размера компании-обладателя информации, числа утечек ПДн).

При анализе выборки по определенному признаку и построении сравнительных диаграмм (такие диаграммы авторы именуют разрезами или распределениями) все утечки, классифицированные по исследуемому признаку как «неизвестные» и с долей менее 5%, исключаются из выборки, после чего совокупность оставшихся утечек принимается за 100% для распределения по вариантам выбранного признака и последующего представления в диаграммах.[10] Такой подход позволяет проиллюстрировать динамические изменения отдельных показателей (долей, приходящихся на утечки, обладающие определенным признаком) более ярко, т.е.

[10] Например, разрез по вектору воздействия, куда входят утечки под воздействием внешних атак и внутреннего нарушителя, не содержит утечек, для которых вектор не удалось определить. То же справедливо для распределений по виновнику, умыслу и другим критериям.

решает исключительно презентационные задачи. Но в случаях, когда доля утечек с признаком, классифицированным как «неизвестный», превышает 5%, представляются отдельные диаграммы.

ЭАЦ регулярно отслеживает обновления по ранее зарегистрированным утечкам.
В ходе такого мониторинга в базу вносится:

- информация об утечках, которые произошли в предыдущие периоды (прошлый год, позапрошлый и ранее),
- обновлённая информация о составе (принадлежности) баз «мега-утечек»,
- уточнённые данные о дате (периоде), когда случилась ранее опубликованная утечка, об объёмах (количестве записей), векторе атаки и т.п.

То есть, при появлении новой информации, данные о количестве, а также векторах воздействия, каналах, суммах штрафов и т.п. утечек за прошлые периоды могут изменяться по сравнению с ранее опубликованными.

Но, как правило, эти данные не оказывают существенного влияния на общие показатели, отраженные в отчетах, а также на обозначенные в исследованиях тенденции.

Глоссарий

Атака – см. компьютерная атака, сетевая атака, вторжение.

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам [Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России. 3 февраля 2012 г.].

Вектор воздействия – критерий классификации в отношении действий лиц, спровоцировавших утечку (в рамках данного отчета InfoWatch).

Различаются действия внешних нарушителей (нарушителей - хакеров и других лиц, как известных, так и не известных) – внешние атаки, направленные против компании, воздействующие на веб-ресурсы, информационную инфраструктуру, носители корпоративной информации с целью компрометации информации, и действия внутренних нарушителей, (сотрудники компании и подрядчики, получившие права доступа к ресурсам компании) атакующих системы защиты изнутри (неправомерный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.), а также допускающих утечки данных своими случайными действиями (бездействием).

Внешняя атака – атака, совершенная внешним нарушителем.

Внутренний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Внешний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Деструктивные действия сотрудников – в рамках данного отчета об утечках информации аналитики InfoWatch к таким действиям относят действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, в том числе сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными] разведками и другими заинтересованными субъектами [ГОСТ Р 50922-2006, статья 2.3.2].

Примечание – Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Инцидент – см. инцидент безопасности, инцидент информационной безопасности, компьютерный инцидент.

Инцидент безопасности (Security incident) – неблагоприятное событие в системе или сети, а также угроза такого события.

Примечание – Иногда используется термин ≪несостоявшийся инцидент≫ для описания события, которое могло обернуться инцидентом при несколько других обстоятельствах [ГОСТ 56205-2014, статья 3.2.106]

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [ГОСТ Р 53114-2008, статья 3.2.7. ГОСТ Р ИСО/МЭК 27001-2006, статья 3.6].

Примечание – Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Канал утечки информации – способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.

На данный момент аналитики InfoWatch выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.

- «Мобильные устройства» – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
- «Съемные носители» – потеря/кража съемных носителей (CD, USB, карты памяти и др.).
- «Сеть (сетевой канал)» – утечка через подключение к сети связи общего пользования, как правило, к сети Интернет (используется сокращение «браузер» для ситуаицй, связанных с отправкой данных через веб-интерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов (cloud), нелегитимная публикация информации на веб-сервисе.
- «Электронная почта» – утечка данных через корпоративную электронную почту.
- «Бумажные документы» – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).
- «IM –сервисы мгновенных сообщений» - утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.
- «Не определено» - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, п.7 ст.2].

Конфиденциальная информация – сведения конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997 г. №188.

В данном отчете (исследовании) авторы относят к таким сведениям информацию, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. Помимо персональных данных, это платежная информация, коммерческие секреты и ноу-хау, а также государственные и военные секреты. В некоторых случаях при анализе полученных сведений определить тип конфиденциальной информации не представляется возможным, поэтому она относится в категории «не определено».

Нарушитель информационной безопасности организации (нарушитель) – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [ГОСТ Р 53114-2008, статья 3.3.5].

В БДУ ФСТЭК России bdu.fstec.ru приведены следующие виды нарушителей/ источников угроз:

- внутренний нарушитель (потенциал низкий, средний, высокий);
- внешний нарушитель (потенциал низкий, средний, высокий).

В данном отчете (исследовании) к категории «нарушитель» авторы относят лицо, которое по ошибке или осознанно (с умыслом – злоумышленник) совершило определенные запрещенные действия, повлекшие утечку информации.

InfoWatch различает два вида нарушителей – «внешний нарушитель» и «внутренний нарушитель», а также шесть категорий нарушителей:

- Внешний нарушитель – Хакер/неизвестное лицо: взломщики компьютерных сетей, в том числе представляющие организованную киберпреступность; владельцы хакерского инструментария (библиотек); взломщики, действующие в политических и социальных целях, - хактивисты; сотрудники иностранных разведок и армий; похитители оборудования с конфиденциальной информацией.
- Рядовой сотрудник.
- Топ-менеджер (руководитель).
- Системный администратор.
- Подрядчик: сторонние исполнители работ по заказу компании, партнеры и внештатные сотрудники.
- Бывший сотрудник.

В рамках исследования топ-менеджеров, системных администраторов, а в отдельных случаях и подрядчиков авторы включают в категорию привилегированных пользователей, то есть пользователей, наделенных повышенными правами доступа к информации. Как правило, действия таких пользователей в информационной системе службами информационной безопасности контролируются слабо либо не контролируются.

Иных пользователей корпоративной информационной системы (рядовых сотрудников) авторы относят к непривилегированным, обычным пользователям.

Неправомерный доступ – см. несанкционированный доступ.

Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа [ГОСТ Р 53114-2008, статья 3.3.6].

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

В данном отчете (исследовании) авторы используют также словосочетание «нелегитимный доступ».

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ Р 50922-2006, статья 2.6.6]

Правонарушение – неправомерное поведение, запрещенное законом под угрозой наступления ответственности общественно вредное или опасное деяние.

Выделяют: преступление (в рамках УК РФ и УПК РФ), административное правонарушение (в рамках КОАП РФ), налоговое правонарушение (в рамках НК РФ).

В отчетах (исследованиях) авторы используют понятие «правонарушение» как родовое (общее) по отношению к преступлению и административному правонарушению.

Привилегированный пользователь – к таким пользователям InfoWatch относит категории лиц, имеющие расширенные права доступа в информационные системы, полномочия по изменению конфигураций и назначения прав администраторов другим пользователям. К привилегированным пользователям относятся руководители различного уровня, системные администраторы, в некоторых случаях подрядчики и другие категории.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации [ГОСТ Р 53114-2008, статья 3.3.11].

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без

согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [98-ФЗ «О коммерческой тайне» п.9 ст.3]

Событие: Возникновение или наличие определенной совокупности обстоятельств [ГОСТ Р 53114-2008, статья 3.2.8].

Примечания:

1. Характер, вероятность и последствия события могут быть не полностью известны.
2. Событие может возникать один или несколько раз.
3. Вероятность, связанная с событием, может быть оценена.
4. Событие может состоять из невозникновения одного или нескольких обстоятельств.
5. Непредсказуемое событие иногда называют «инцидентом».
6. Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками [ГОСТ Р 53114-2008, статья 3.3.10].

В данном отчете (исследовании) InfoWatch к категории «утечка информации» относится событие, когда в результате умышленных или неумышленных действий внутреннего или внешнего нарушителя обладатель информации ограниченного доступа (компания) утрачивает контроль над этой информацией.

Умышленная (злонамеренная) утечка информации – InfoWatch понимает под ней такую утечку, когда пользователь, работающий с информацией ограниченного доступа, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду, или руководствовался иными мотивами (месть, зависть, личная неприязнь и т.д.). При этом в результате таких действий контроль над информацией со стороны ее обладателя был утрачен. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.