Россия.
Утечки информации ограниченного доступа в 2021 году

© Экспертно-аналитический центр InfoWatch. 2022 г.

Оглавление

Только факты 3
Сокращения 4
Аннотация 4
Результаты исследования 5
Заключение и выводы 17
Мониторинг утечек на сайте InfoWatch 19
Методика 20
Глоссарий 23

Только факты

- ✓ Доля утечек с применением средств автоматизации в России выросла с 68% в 2018 г. до 86% в 2021 г.
- ✓ Количество скомпрометированных записей персональных и платежных данных увеличилось на 20%.
- ✓ Девять из десяти утечек содержат персональные данные.
- ✓ Доля утечек, вызванных внешними нарушителями, за четыре года выросла с 9% до 25%.
- ✓ В 2021 году более 82% всех утечек и 76% утечек по вине внутреннего нарушителя являются умышленными.
- ✓ Более 1/3 всех утечек пришлись на высокотехнологичную сферу.

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
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ЭАЦ	Экспертно-аналитический центр ГК ИнфоВотч

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch провел ежегодное исследование утечек информации ограниченного доступа из российских компаний и госорганизаций на основе данных из открытых источников. Отмеченные в 2021 году показатели сравниваются в различных разрезах с показателями предшествующих лет (2018-2020 гг.), чтобы выявить и проследить основные тенденции.

Результаты исследования

За 2021 г. экспертно-аналитический центр InfoWatch зарегистрировал 331 утечку информации ограниченного доступа из коммерческих компаний, органов власти и государственных организаций в России. Это на 40,8% меньше, чем в 2021 г., и на 46,4% меньше, чем в аномальном 2019 г., когда было зарегистрировано наибольшее количество утечек за всю историю исследований InfoWatch. Данные о количестве зарегистрированных утечек в России представлены на Рисунке 1.

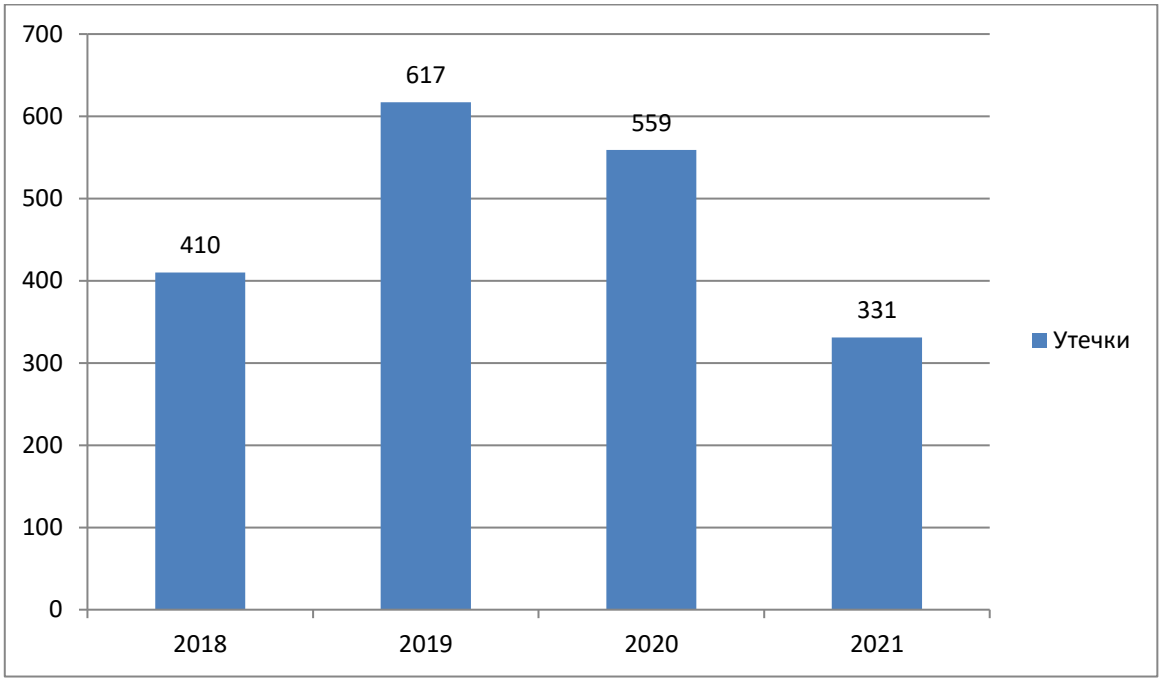

Рисунок 1. Число зарегистрированных утечек: Россия, 2018-2021 гг.

> *Коммерсантъ: База данных 1,3 млн российских владельцев автомобилей Hyundai выставлена на продажу на теневых форумах. В ней содержатся в том числе адреса пользователей, информация об автомобилях и заказе запчастей. Злоумышленники могут использовать данные для угона автомобилей, также их владельцам стоит ожидать сообщений от спамеров, предупреждают эксперты по кибербезопасности.*

> *Znak: В Челябинской области сотрудник одного из банков обвиняется в нарушении банковской тайны. По версии следствия, подозреваемый передал неустановленному лицу информацию о 100 вкладчиках и получил за это от него не менее 200 тыс. рублей.*

Наметившееся вскоре после начала пандемии снижение количества зафиксированных в открытых источниках инцидентов отчетливо проявилось в 2021 г. Вероятно, во многом из-за того, что в пандемию был ослаблен контроль за сотрудниками, многие инциденты могли оказаться в тени и возникли новые возможности для злоумышленников. 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) скопировать защищаемые данных. Как следствие, они более успешно боролись с утечками.

На Рисунке 2 дано распределение утекших записей за четыре года (ПДн и платёжная информация). За 2021 г. в открытых источниках найдена информация об утечке более 80 млн записей ПДн и платежной информации. Это примерно на 20% больше, чем в 2020 г., но в два с лишним раза меньше, чем в аномальном с точки зрения утечек 2019 г. Вероятно, в 2020-2021 гг. черный рынок, из которого, как известно, черпают данные разного рода злоумышленники для реализации мошеннических схем, не испытывал особой нехватки информации о гражданах – помимо свежей информации, в Дарквебе активно распространялись базы данных и их фрагменты из утечек прошлых лет.

Таким образом, в 2021 году в России наметилась тенденция роста количества утечек персональных данных и платёжной информации.

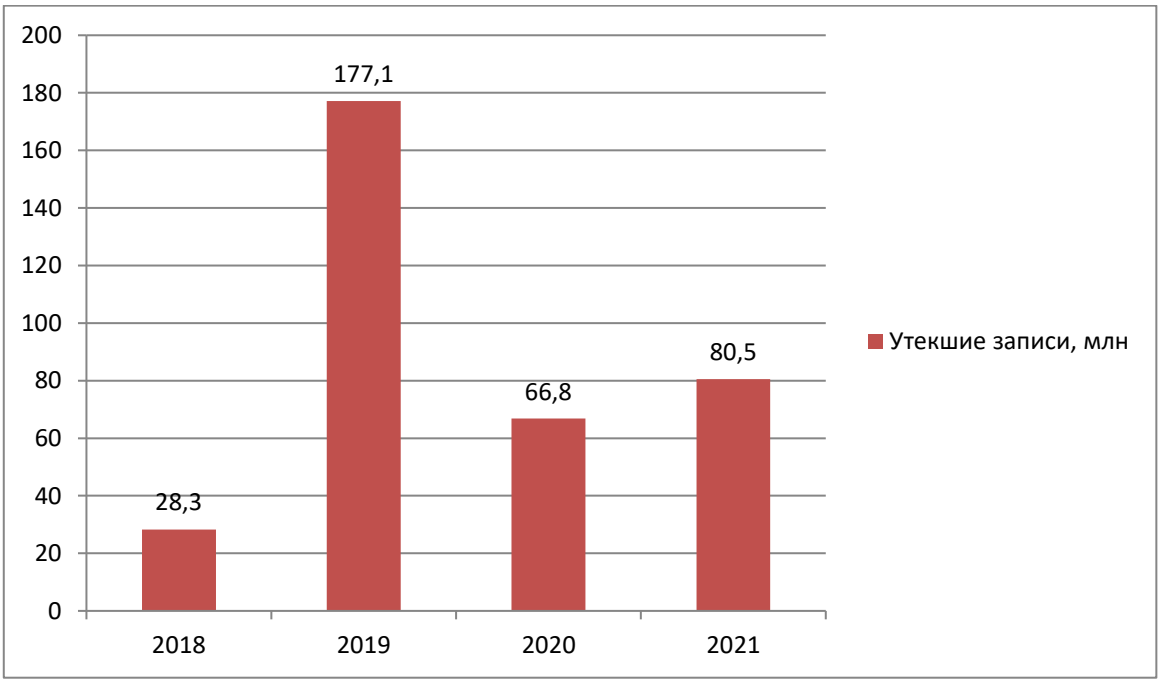

Рисунок 2. Количество утекших записей: Россия, 2018-2021 гг.

Полагаем, что свежая информация, как правило, была нужна злоумышленникам в тех случаях, когда требовалось устроить фишинговые атаки, прикрываясь актуальной повесткой. Речь прежде всего идет о мошеннических схемах, связанных с пандемией: вакцинация, QR-коды, социальные выплаты и т.д.

Кроме того, дельцы подпольного рынка данных стали активнее заниматься обогащением ранее сформированных баз, то есть включали дополнительные сведения в коллекции файлов с ПДн. Таким образом на стороне организованной преступности постепенно идет формирование обширных баз данных с цифровыми профилями граждан России. Наличие в базах, сформированных криминалитетом, данных о человеке по десяткам параметров, включая базовую информацию из документов, а также политические предпочтения, социальные связи, имущественное положение и т.д., повышает риски мошенничества и может привести к тяжелым последствиям, вплоть до

формирования «цифровых двойников», которые возможно использовать как для финансовых махинаций, так и в экстремистских целях. Задачу злоумышленникам может облегчить недостаточное внимание к защите государственных баз данных, которые в результате бурного развития цифровизации в последние годы аккумулировали самый широкий спектр сведений о людях.

На Рисунке 3 можно проследить, что в России снижается доля утечек по вине внутренних нарушителей. На наш взгляд, это связано, во-первых, с активизацией хакеров и других внешних нарушителей на фоне успехов в цифровизации – когда структурированных хранилищ информации становится больше, это неизбежно привлекает киберпреступников. Во-вторых, во время борьбы с новой коронавирусной инфекцией и массового перевода сотрудников на удаленную работу могла существенно вырасти латентность инцидентов внутреннего характера: компании, не успевшие или не захотевшие внедрить средства контроля за сотрудниками, оставались в неведении о многих активностях персонала, работающего из дома. Причем активность, ведущая к утечкам, не обязательно может быть умышленная – от ошибок, тем более в новых на тот момент условиях (между кухней и детской), никто не застрахован В-третьих, в пандемию значительно усложнился вектор ряда инцидентов, все чаще приходится говорить об использовании злоумышленниками многоступенчатых схем похищения информации, когда в сговор вступают внутренний и внешний злоумышленник и, в результате внутренний нарушитель создаёт условия для успешных действий внешних, или совершает копирование и передачу сам, переводя акцент на них, тем самым избегая внимания служб безопасности, а продажу данных осуществляют его «сотоварищи» под видом хакеров.

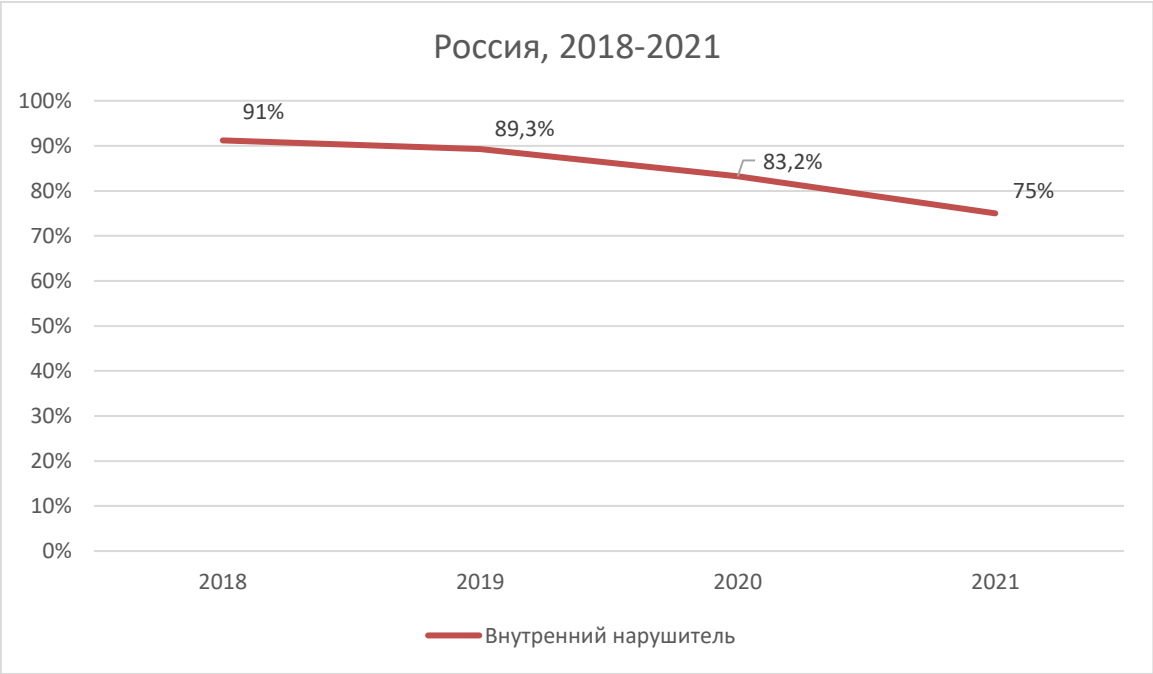

Рисунок 3. Динамика доли утечек по вине внутренних нарушителей: Россия, 2018-2021 гг.

Таким образом, можем обоснованно полагать, что внутренние нарушители в России все еще остаются главной угрозой для информационных активов бизнеса и государственных структур. Но чтобы минимизировать эту угрозу, у компаний и организаций есть все возможности. Необходимо внедрять и правильно настраивать современные системы выявления утечек и контроля действий персонала, средства управления доступом, продвинутую аналитику на основе машинного обучения и, конечно, проводить регулярные мероприятия для повышения цифровой грамотности сотрудников.

Отметим, что в пандемию резко выросла доля утечек умышленного характера – с 58% в 2019 г. до 83% в 2020-2021 гг. (Рисунок 4). К этому привело сочетание нескольких факторов: рост хакерской активности, ослабление контроля за персоналом в условиях удаленной работы, повышение ценности ПДн и другой конфиденциальной информации на черном рынке в условиях цифрового развития (с учётом первоначальных ошибок и неопределенности при переводе ряда сервисов на дистанционную работу, без личной явки и подтверждения). Кроме того, в пандемию выросли в объёмах или возникли новые обширные источники персональных данных (сведения о заболевших COVID-19 и о вакцинированных и т.д., информация о социальной поддержке в условиях пандемии), значительно расширились базы ряда востребованных в пандемию сервисов, в первую очередь служб доставки еды. В таких условиях стало намного больше охотников за информацией как за пределами информационного контура организации, так и внутри него.

Рисунок 4. Динамика доли умышленных утечек: Россия, 2018-2021 гг.

Одновременно выросла доля умышленных нарушений по вине сотрудников (Рисунок 5). В 2020 г. она составила почти 80%. Правда, в 2021 г. она несколько снизилась, но связано это было, скорее всего, с повышением латентности внутренних инцидентов – полагаем, что большинство из них просто остались незамеченными.

Рисунок 5. Динамика доли умышленных утечек внутреннего характера: Россия, 2018-2021 гг.

Ниже, на Рисунке 6, показано распределение утечек по типам скомпрометированных данных. **За четыре года доля утечек ПДн выросла с 80% до без малого 90%**. Персональные данные гражданина за последние годы из сухих сведений трансформировались в личный актив, а цифровой профиль человека стал все чаще рассматриваться обществом как ценный артефакт, требующий защиты.

Рисунок 6. Распределение утечек по типам данных: Россия, 2018-2021 гг.

В условиях низкой цифровой культуры граждан и при отсутствии механизмов защиты персональные данные становятся удобным объектом монетизации в цифровую эпоху. В ряде случаев, имея такую информацию, мошенники могут оформить займ или выплату, также они могут организовать фишинговую атаку или просто продать ПДн заинтересованным лицам на теневых форумах.

Вместе с тем, практически на нет сошли утечки платежной информации (данных банковских карт). Можно сделать вывод, что банковская инфраструктура в целом

достаточно хорошо защищена от посягательств, о чем свидетельствуют результаты киберучений, организованных Центробанком. Поэтому платежные данные злоумышленники стараются выведать посредством фишинговых атак, получив определенный набор персональных данных жертвы.

Также отметим, что в 2021 г. выросла доля утечек информации, относящейся к категории «коммерческая тайна». Это отражает тренд на восстановление экономики, несмотря на в пандемию, и повышение роли конкурентной борьбы. Кроме того, в России становится больше коммерческих секретов, интересных международной киберпреступности – группировкам, действующим в интересах ряда стран, в том числе «недружественных государств».

Распределение утечек по виновникам представлено ниже на Рисунке 7. Изменение долей в соответствующих разрезах во многом коррелирует с изменением распределения по вектору атак (напомним, что на Рисунке 3 приведены доля утечек в результате внутренних нарушений). В результате всплеска хакерской активности, на фоне кибервойн и проблем с контролем за информационными ресурсами в пандемию доля утечек по вине персонала снизилась. На долю хакеров и неизвестных лиц пришлось почти 1/3 всех утечек, зарегистрированных в России за 2021 г. Также нельзя забывать оросте латентности внутренних нарушений, о чем мы сказали выше.

Есть и позитивный тренд. Он связан со снижением в 2021 г. доли утечек по вине привилегированных пользователей (руководители и системные администраторы). Хотя и здесь можно предположить, что большую роль сыграл рост латентности нарушений, в т.ч. связанный с трудностями контроля, особенно при дистанционной работе (часто активность переносилась на личные устройства).

Рисунок 7. Распределение утечек по виновнику: Россия, 2018-2021 гг.

Далее на Рисунке 8 приведено распределение утечек по каналам. **Можно заметить, что если в 2018 г. в России преобладали утечки посредством кражи или утери бумажных документов, то в последующие годы на первый план вышли утечки через Сеть, также резко выросла доля утечек через мессенджеры (IM).**

Доля утечек информации без применения средств автоматизации (компрометация данных в результате кражи или потери бумажных документов, а также в результате кражи или потери средств хранения) в 2021 г. составила 15,8%. Это почти в три раза меньше, чем в 2018. Такая динамика отлично показывает, как всего за несколько лет мир стал цифровым. Естественно, помимо удобств, он принес новые риски, которые пока не удается минимизировать.

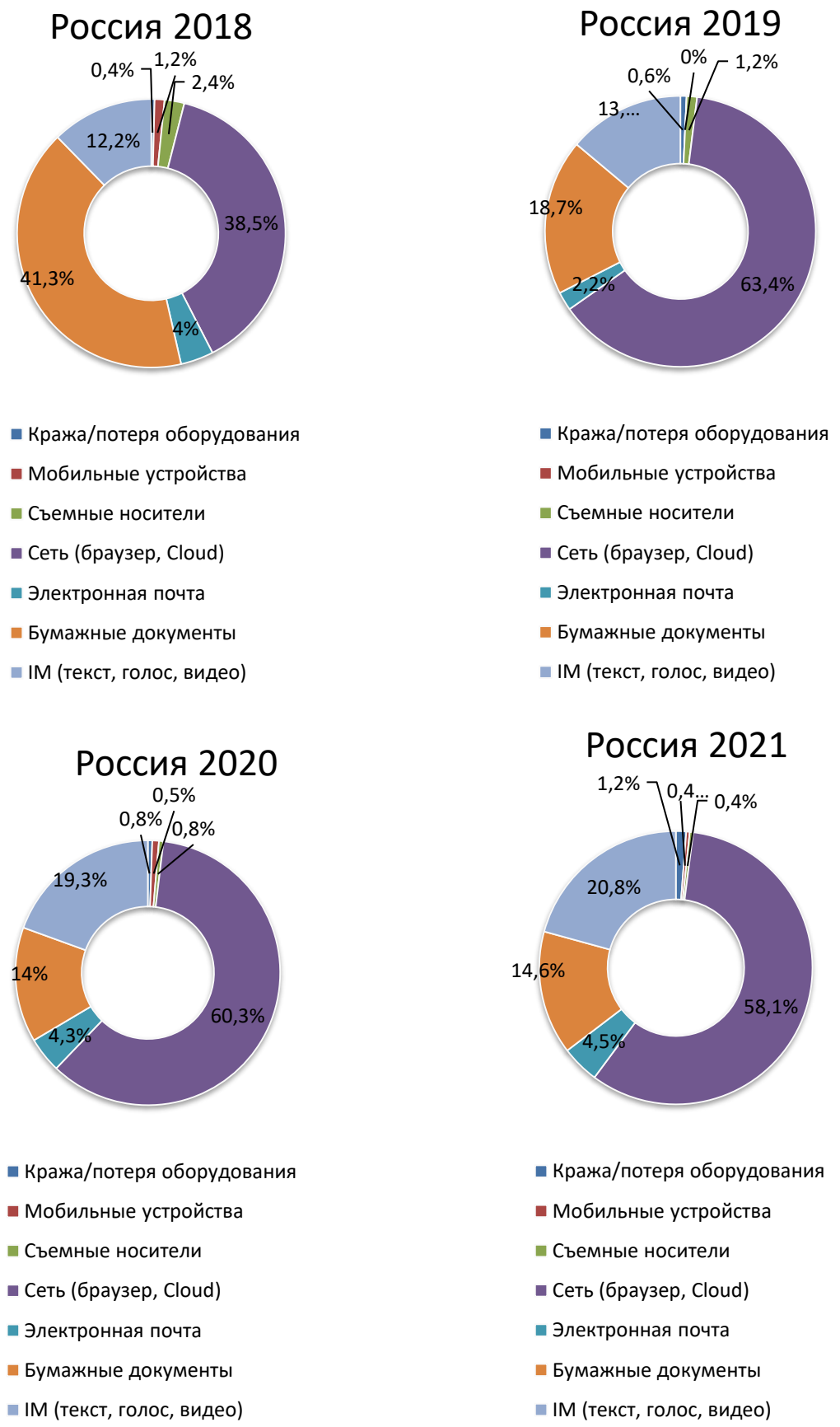

Рисунок 8. Распределение утечек по каналам: Россия, 2018-2021 гг.

На Рисунке 9 представлено распределение зарегистрированных утечек по отраслям. Обращает на себя внимание тот факт, что **в 2021 г. резко выросла доля утечек в высокотехнологичном секторе (ИТ-компании, операторы связи, ИТ-сервисы и т.д.). Более трети всех утечек пришлись на эту сферу.** На наш взгляд, такое положение связано со стремительным развитием цифровых услуг и накоплением массивов персональных данных в структурированных хранилищах – не все ИТ-компании хорошо подготовились к защите ПДн своих клиентов и сотрудников. Кроме того, активизировались внутренние злоумышленники в операторских компаниях – наши отчеты по судебной практике показывают, что именно менеджеры сотовых операторов чаще всего продают данные.

Рисунок 9. Отраслевое распределение утечек, Россия, 2018-2021 гг.

Заключение и выводы

Пандемия и связанная с ней коренная перестройка форм реализации ряда процессов стали главными факторами формирования картины утечек в 2020-2021 гг. Перевод миллионов сотрудников на удаленную работу не позволил быстро адаптировать системы защиты информации под новую реальность (за редким исключением). Многие компании не успели, не смогли или не захотели внедрить средства контроля дистанционных сотрудников, в результате чего, как мы считаем, большой пласт инцидентов ушел в тень и не все из них сразу появились на чёрном рынке данных.

Параллельно с проблемами контроля удаленной работы в 2021 г. нарастала хакерская активность, многие компании испытывали колоссальное давление со стороны киберпреступников. В условиях стремительной цифровизации последних лет возникли десятки и сотни структурированных хранилищ информации, ставших желанными объектами для злоумышленников. В то же время продолжился рост ценности информации ограниченного доступа, прежде всего персональных данных, на черном рынке. И здесь часто сходятся интересы хакеров и внутренних нарушителей. В результате мы все чаще вынуждены говорить о тенденции роста и выхода на первый план гибридного вектора атак.

Выводы:

1. Растёт доля утечек, вызванных действиями внешних нарушителей (согласно открытым данным). За четыре года она увеличилась почти в три раза – до 25%. Это вызвано всплеском хакерской активности, успехами ряда компаний во внедрении средств защиты от внутренних нарушителей, а также ростом латентности нарушений внутреннего характера, трудностями классификации утечек – опубликованные в Дарквебе по умолчанию считаются внешними, но какова среди них доля внутренних или гибридных неизвестно. То есть на долю внутренних нарушителей приходится 3 их 4 опубликованных утечек.
2. В пандемию с 58% до 83% выросла доля утечек умышленного характера, что связано с повышением ценности информации, ослаблением контроля над персоналом и формированием значительного числа новых структурированных баз данных, необходимых для дистанционных (электронных) сервисов, ставших желанными объектами для злоумышленников.
3. Небольшой рост доли умышленных утечек по вине внешних нарушителей (на 3%) в 2021 году вызван, прежде всего, ростом латентности внутренних нарушений (в 2021 году доля утечек внутреннего характера составляла 76%).
4. За четыре года на 12% выросла доля известных утечек по вине привилегированных пользователей. Некоторое снижение доли утечек по вине персонала возможно соотнести с ростом хакерской активности, а также повышением латентности внутренних нарушений (трудоёмкости их выявления и расследований причин утечек).
5. В 9 из 10 утечках фигурируют персональные данные. ПДн, они становятся всё более привлекательными для злоумышленников.
6. Стремительное развитие цифровизации привело за последние четыре года к сокращению доли утечек без использования средств автоматизации в три раза

(компрометация бумажных документов, кража и потеря оборудования), то есть наблюдается резкий рост потерь данных в электронном (цифровом) виде.

7. Вдвое – с 17% до 34% - выросла доля утечек из компаний сферы «Высокие технологии». Это связано с развитием цифровизации, появлением большого числа новых ИТ-сервисов и, по-видимому, недостаточным вниманием к защите собственных ресурсов.

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
- VK
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

© InfoWatch

Полное воспроизведение, опубликование материалов запрещено.

Цитирование возможно только при указании ссылки на источник.

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. Источником для этой базы являются публичные сообщения[1] о случаях утечек информации из учреждений, организаций, предприятий любых организационных форм и форм собственности, включая органы государственной власти и управления, а также данные из некоторых закрытых и условно-закрытых источников (форумы, чаты, каналы).

В настоящий момент количество записей в базе превышает 20 тысяч.

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

Исследования ЭАЦ, в основном, ориентированы на анализ сообщений об утечках данных на английском и русском языках. Во многом с этим связана большая доля в базе информации об утечках в России и сообщений об утечках из компаний англосаксонских стран и Европы. Для обеспечения и увеличения полноты охвата также используются источники на арабском, японском, немецком, французском, испанском и итальянском языках. 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 каждому сообщению присваивается 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,
- ссылка на источник сообщения,
- дата публикации сообщения,
- название предприятия (организации, учреждения);
- государство (страна),
- сфера деятельности обладателя информации (отрасль),
- направление деятельности (коммерческая, некоммерческая),
- примерный размер организации (малая, средняя, крупная)[2],
- размер причиненного в результате утечки ущерба[3],
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- субъект[4], непосредственно допустивший утечку.

Выделяются следующие сферы деятельности (отрасли, отраслевые группы):

- банки, финансовые и страховые компании,
- медицина,

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

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

[3] 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.

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

- 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[5] (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.),
- вектору воздействия («внешний», «внутренний», «не определено», также 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 количество скомпрометированных записей, содержащих только 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.

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

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 и 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.[6] Такой подход позволяет проиллюстрировать динамические изменения отдельных показателей (долей, приходящихся на утечки, обладающие определенным признаком) более ярко, т.е. 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»,

[6] 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.

- 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).

ГАС «Правосудие» - Государственная автоматизированная система Российской Федерации.

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).

Запись в ГАС «Правосудие» - запись на сайте https://bsr.sudrf.ru/, включающая информацию об одном судебном решении.

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 браузер (отправка данных через веб-интерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, 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.

Критическая информационная инфраструктура Российской Федерации — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

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».

Нарушение с применением средств автоматизации – нарушение положений (требований) статей Кодекса об административных нарушениях РФ или Уголовного кодекса РФ с использованием компьютера, средств связи и сети Интернет.

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]

Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

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.

Субъекты критической информационной инфраструктуры — государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Судебное дело – совокупность судебных решений всех инстанций, которые относятся к одному факту нарушения Кодекса об административных нарушениях или уголовного кодекса РФ.

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.