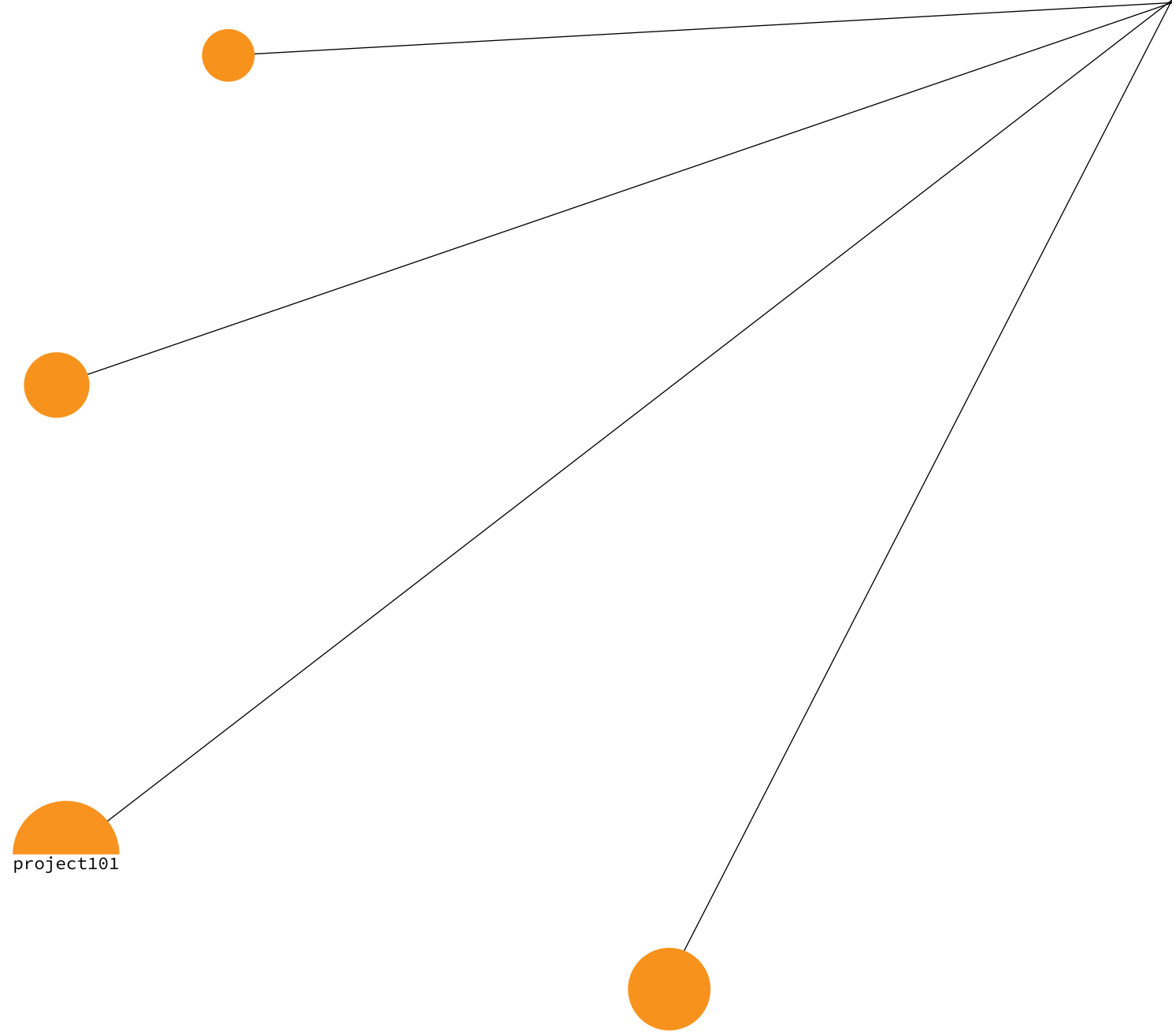


Кибератаки в судах

Мы рассмотрели более 100 дел в российских судах, где упоминалась кибератаки и выбрали из них наиболее показательные. В подборку вошло 30 гражданских и 11 административных споров о персональных данных. Для юристов мы привели цитаты из 17 решений для копирования в Ваши позиции, а также матрицы ссылок на нормативно-правовые акты, которые Суды использовали при принятии актов. Для специалистов по информационной безопасности мы сформировали схемы построения процессов, которые могли бы помочь оператору отстоять свои интересы после инцидента

В нашем Telegram-канале также есть серия материалов по обработке персональных данных. Вы можете связаться с нами через сообщения канала, а подписка на него станет лучшей поддержкой для нас

Содержание:

Авторы:
Илья Башкиров
Игорь Линич

Введение: факты

Самый популярный сценарий ссылки на кибератаку в суде – защита от ответственности за убытки или просрочку, ставшие следствием кибератаки.

Мы не нашли ни одного дела о **киберстраховании**

1 раз кибератаку признали **форс-мажором** !

В 2025 году кибератака перестала исключать **ответственность за утечку персональных данных**. Это – серьезное изменение в практике по 13.11 КоАП

99% успеха при ссылке на кибератаку в защите – это взаимодействие оператора с его контрагентом и стремление исполнить условия сделки. Именно в таком случае кибератаку могут признать форс-мажором и **исключить неустойки и компенсации**

И в административном, и в гражданском процессе суды считают кибератаки **нормальным и известным деловым риском**

У авторов есть Telegram-канал **@project101_LF**

Кибератаки в простых вопросах

*Кибератака – это **форс-мажор**?* ?

Ответ: **да**, ее можно признать форс-мажором, но только при условии грамотной работы с ее причинами и последствиями. Подробнее – стр. 7

*Кибератака исключает **ответственность за утечку ПДн**?* ?

Ответ: **нет**. Суды считают, что, собирая данные, Оператор берет на себя публично-правовую обязанность по их защите. Анализ дел на стр. 14-16

*Провайдер отвечает за **все сбои** на своей стороне?* ?

Ответ: **нет**, только за те сбои, которые предусмотрены Договором. Суды в таких делах внимательно анализируют тип атаки и обязанности провайдера. Рекомендации на стр. 12

Можно ли снизить штрафы за просрочку по причине кибератаки? ?

Ответ: **да, можно**, но нужно соблюсти некоторые требования по реагированию на инцидент. Они перечислены на стр. 8

Общий обзор

*За 2022-2025 гг. 13 делах кибератака упоминалась, как причина **невозможности исполнения** обязательства в принципе или в установленный договором срок. 7 раз на кибератаку ссылались, как на причину **просрочки процессуального или административного действия**. 5 раз исковое заявление подавалось **с целью взыскания ущерба**, причиненного кибератакой, а также еще в 3 делах такой ущерб взыскивался **с провайдера хостинга**. Наименее популярный сценарий – это ссылка на кибератаку как на **причину утраты информации**, имеющей юридическое значение (2 дела)*

В подборку не вошли дела по ст. 13.11 КоАП – причина в том, что мы не можем объективно установить их количество. Скорее всего, это самый популярный сценарий ссылки на кибератаку. Мы разобрали 9 дел на стр. 14

Последствия кибератаки:

Обычно результатом кибератаки (*извне или изнутри организации*) является либо утечка информации, либо срыв бизнес-процессов. Утечка приводит к гражданско-правовым (*штрафы и убытки по NDA*) и административно-правовым последствиям (*штрафы за утечку ПДн*). Срыв бизнес процессов сопровождается убытками, неустойками и принудительным взысканием в гражданско-правовом споре. Утрата информации приводит к неэффективности доказывания и оспариванию административных действий

Срыв бизнес-процессов

Исполнение

Сбой в системах иногда приводит к невозможности или затруднительности исполнения основного обязательства по договору. Так формируется «тело долга». Юридический инструмент – истребование денежных средств или принудительное исполнение

Убытки

Сценарий спора – кибератака на Сторону А привела к убыткам Стороны Б. Ими могут быть затраты на восстановление инфраструктуры в случае атаки типа supply chain, необходимость искать альтернативного поставщика или упущенная выгода ввиду простоя бизнес-процессов

Неустойки

Нарушение бизнес-процессов приводит к срыву сроков поставки/предоставления или оплаты товаров, работ или услуг. В результате стороны договора вступают в спор о выплате неустоек, предусмотренных договором

Утечка информации

Гражданско-правовые последствия

Утечка информации, доступ к которой ограничен соглашением между сторонами (NDA), может повлечь предусмотренные им штрафы и компенсации

Административно-правовые санкции

Законодательство о персональных данных предусматривает ответственность за их утечку. При этом предусмотрено, что основанием для привлечения Оператора к ответственности может быть его бездействие в вопросе защиты информации

§ Исполнение обязательств и неустойки

Кибератаки регулярно приводят к сбоям в цепочках поставок. Нарушение срока поставки, сдачи-приемки или оплаты, скорее всего, приведет к штрафу (неустойке) оператора за просрочку. Но можно ли сослаться на кибератаку, как уважительную причину для нарушения срока исполнения обязательств?

Развивая эту идею, некоторые операторы приходят к более радикальной мысли: а может, вообще не исполнять обязанности, которые стали излишне затруднительными после кибератаки? В таком случае кибератаку пытаются признать обстоятельством непреодолимой силы, исключающим ответственность – форс-мажором. Однако на практике это оказывается достаточно затруднительным ввиду специфичной позиции судов

Матрица нормативно-правовых ссылок:

*П. 8 ПП ВС от 24.03.2016 №7: форс-мажорное обстоятельство является **чрезвычайным** (его нельзя было предугадать) и **неотвратимым** (обычный участник рынка не мог бы его предотвратить)*

П. 9 ПП ВС от 24.03.2016 №7: форс-мажор освобождает от убытков, неустоек и штрафов, но не прекращает само обязательство. После прекращения форс-мажорных обстоятельств обязательство должно быть исполнено, но без штрафов за просрочку. При этом контрагент пострадавшей от кибератаки стороны может по своему желанию отказаться от договора, если просрочка сделала исполнение бессмысленным для него

Ч. 3 ст. 401 ГК РФ: сторона освобождается от ответственности в случае, если такая ответственность была вызвана форс-мажором

Ст. 333 ГК РФ: неустойка по договору в (не-таких-уж-и) исключительных случаях может быть снижена

Таким образом, кибератака не может быть основанием **не исполнять обязанности по договору в принципе**

При этом суд может снизить неустойки и штрафы или вовсе отказать в их взыскании, если посчитает, что оператор, подвергшийся кибератаке, стремился исполнить обязательства не смотря на технические трудности. В таких случаях акцент спора смещался не на доказывание наличия/отсутствия кибератаки, а на обоснование добросовестного поведения оператора, как стороны сделки

Case Study: исполнение обязательств

Некоторые организации считают, что кибератака, повлиявшая на исполнение обязательств между сторонами, позволяет оказаться от их исполнения в принципе. Ниже рассмотрим примеры таких дел

Факт кибератаки **не освобождает** от исполнения обязательств **сам по себе**

А40-129508/2022 *Постановление 9ААС от 29.03.2023*

Ответчик (*агент*) продавал продукцию Истца (*принципала*) по агентскому договору и должен был отчислять ему комиссию. Из-за кибератаки информационная система Ответчика была заблокирована, а данные – повреждены. В результате он не выплатил комиссию по договору и сослался на кибератаку, как на форс-мажор. Истец (*Принципал*) обратился в Суд с требованием взыскать сумму комиссии. **Суд удовлетворил требование** в полном объеме.

«*...обстоятельство признается непредотвратимым, если любой участник гражданского оборота, осуществляющий аналогичную с должником деятельность, не мог бы избежать наступления этого обстоятельства или его последствий. Вместе с тем, Ответчиком не доказана причинно-следственная связь между указанными им обстоятельствами и наличием долга, а также обязанностью его оплатить. Более того, указанные ответчиком доводы документально не подтверждены*»

#DDoS

Суды считают, что **сделка имеет реальную природу и связана с действиями в «аналоговом мире»**. Поэтому суды в в первую очередь определяют, насколько сильно сбой в информационной среде влияет на **фактическую исполнимость условий договора**

А75-13132/2025 *Решение АС Ханты-Мансийского АО– Югры от 21.10.25*

Арендатор должен был регулярно перечислять плату за аренду земельного участка Арендодателю. Информационная система Арендатора подверглась атаке и была временно заблокирована. Из-за этого регулярный платеж был осуществлен на 5 дней позже. Арендодатель направил иск о взыскании неустойки за просрочку, и **Суд его удовлетворил**.

«*Ответчик ссылается на массовую хакерскую атаку на IT-инфраструктуру компании в конце марта 2025 года, однако данный довод не может быть признан обстоятельством непреодолимой силы (форс-мажором), поскольку он не подтвержден официальными документами, не исключал возможность получения почтовой корреспонденции, не препятствовал выполнению обязанности по контролю за своевременным исполнением финансовых обязательств, включая использование резервных каналов связи и непосредственного взаимодействия с кредитными организациями*»

#DDoS #отказ_системы

Вывод:

В случае, если кибератака делает невозможным временное исполнение договора, сторона, подвергшаяся кибератаке, должна принять все необходимые действия для того, чтобы исполнить договор. Среди них – перевод исполнения договора в аналоговый режим.

project101

Case Study: DDoS

Исследуя материалы и обстоятельства дела, суды также учитывают и тип кибератаки и ее характеристики, в том числе, оценивая масштаб последствий

DDoS – не оправдание

Суды определяют степень влияния кибератаки на бизнес процессы по типу атаки, затронутым процессам и продолжительности сбоя

А33-25417/2025 *Решение АС Астраханской области от 04.12.2025*

Оператор в защите сослался, что не мог выполнить условий сделки из-за того, что его системы были повреждены DDoS атакой. Суд удовлетворил иск, поскольку посчитал, что Оператор мог предупредить своего потребителя о сбое в системах и оказать услугу иным образом

«…*сам характер технического сбоя не свидетельствует о полном отказе в обслуживании потребителя интернет-услуги, тем самым представленная Оператором информация о наличии технических сбоев с достоверностью не устанавливает и не подтверждает, что направленный Фондом в адрес заявителя запрос не был или не мог быть получен, учитывая, что оператором АО "Калуга Астрал" подтвержден факт передачи транспортного сообщения в адрес страхователя 04.04.2025.Следовательно, учитывая данные оператора АО "Калуга Астрал", заявителем не представлено в достаточной степени подтверждающих доказательств неполучения запроса потребителя*»

#DDoS

В тех случаях, когда у оператора была возможность исполнить обязательство или получить информацию альтернативным способом, ссылка на кибератаку в защите неэффективна

А24-4158/2024 *Решение АС Камчатского края от 07.03.2025*

Оператор требовал уменьшения задолженности ввиду неких неучтенных обеспечительных платежей, данные о котором были уничтожены в результате DDoS-атаки. Суд отказал и отметил, что данные о платежах хранятся не только на ресурсах Оператора, но и могут быть затребованы у банка

«*Доводы ответчика о невозможности представить соответствующие доказательства со ссылкой на DDoS-атаку и утрату данных расцениваются судом критически, поскольку данное обстоятельство не лишало ответчика возможности запросить соответствующее платежное поручение в кредитном учреждении, где у него открыт расчетный счет, либо представить выписку по счету в подтверждение соответствующего перечисления*»

Дополнительно изучается логическая сопоставимость типа кибератаки и последствий, заявленных оператором

А60-65925/2023 *Решение АС Камчатского края от 07.03.2025*

Оператор указывал, что реклама казино на его сайте появилась в результате кибератаки. Суд посчитал, что такой результат кибератаки является не только недоказанным, но и нелогичным

«*Какие-либо доказательства, подтверждающие частный вывод сотрудника общества, сделанный им в служебной записке о том, что наличие ошибки «502 Bad Gateway» явилось следствием именно DDoS-атаки, в материалы дела не представлены, например, выписки из журнала о доступности/недоступности сайта*»

Case Study: форс-мажор

Ссылка на невозможность исполнения ввиду кибератаки является неэффективной, если существует разумный альтернативный способ исполнить обязательство.

Да, кибератака может быть форс-мажором

Если исполнение обязательств невозможно без информационной системы, а альтернативные пути его исполнения неразумны (по техническим или экономическим причинам), кибератака может быть признана форс-мажором

A15-1085/2022 *Постановление 16AAC от 15.08.2023*

Сбой информационной системы заправок привел к невозможность отпускать топливо по топливным картам. Организация, закупившая топливные карты, решила взыскать штраф за неисполнение обязательств, предусмотренный договором.

Но Суд (в апелляции) указал, что **кибератака является форс-мажорным обстоятельством** и отказал истцу во взыскании штрафа.

«*Таким образом, временная невозможность поставки топлива заказчику по топливным картам на некоторых заправках вызвана не действиями (бездействием) общества, а сбоем в работе системы, что является форс-мажорным обстоятельством и является основанием для освобождения ответчика от применения к нему меры ответственности в виде штрафа*»

#DDoS #отказ_системы

На такую позицию Апелляционного суда повлияло **два фактора**:

1. «**Масштаб**» **кибератаки и** «**масштаб**» **неисполнения обязательств были идентичны**. Владелец сети заправок указал на то, что топливо нельзя было получить только на некоторых заправках. На всех остальных – пожалуйста. Иными словами, Владелец сети не утверждал, что кибератака освобождает его от всех обязательств в принципе, и он старался исполнять их по мере фактической возможности.
2. Исполнение договора было основано на **взаимодействии при помощи информационной системы**. У стороны, подвергшейся кибератаке, определенное время отсутствовала фактическая возможность исполнить обязательства именно по технической причине. Но сторона приняла все действия, чтобы устранить эту техническую неисправность.

Вывод:

Да, практика позволяет признать кибератаку форс-мажорным обстоятельством, но только в «локальном масштабе». При этом стороне следует доказать наличие разумных мер противодействия кибер-угрозам

Перефразируем: кибератака это не «катастрофа», а «осложнение». Сторона **должна стремиться исполнить договор по мере возможностей**, возможно, используя иные пути исполнения обязательств. Но у Суда может возникнуть вопрос: «а если система так важна, то почему вы ее не защищали?» – следует запастить доказательствами обеспечения ИБ

Выводы: обязательства и неустойки

Для того, чтобы кибератака была признана обстоятельством, исключающим или снижающим ответственность, оператор обязан доказать не только факт кибератаки, ее непредвиденный и неотвратимый характер, но и свое стремление исполнить обязательство альтернативными методами

Кризисное исполнение:

Мы предлагаем предусматривать в бизнес-процессах и договорах «кризисное исполнение». Под ним мы пониманием способ выполнения обязанностей в обход поврежденных информационных систем. Схематически он может быть представлен следующим образом:

Для закрепления кризисного исполнения **в договоре** можно предусмотреть:

1) альтернативный способ направления юридически значимых **сообщений** между заказчиком и исполнителем в случае сбоя информационных систем;

2) порядок **уведомления** о сбоях в информационных системах и кибератаках и способы подтверждения факта их наступления;

3) нештрафные периоды и **отсрочки**, предоставляемые для устранения последствий кибератаки;

4) обязанности пострадавшей от кибератаки стороны по восстановлению устойчивости информационных систем

NB *В любом случае действия по уведомлению контрагента о кибератаке, предложению альтернативных сроков и методов исполнения обязательств можно считать обязательными для признания кибератаки обстоятельством, снижающим или исключающим ответственность*

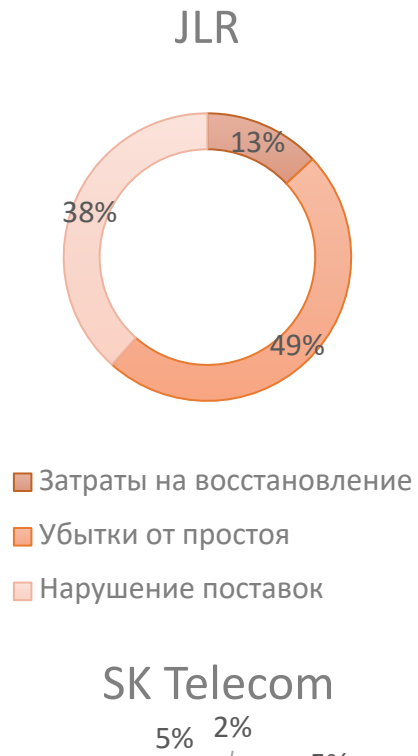
§ Убытки

Ст. 15 ГК РФ устанавливает право Лица требовать полного возмещения убытков, вызванных нарушением его права. Статья разделяет убытки на ***реальный ущерб*** *и* ***упущенную выгоду****.*

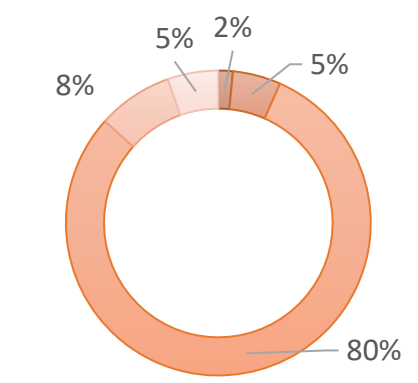
Структура убытков от кибератаки:

Реальный ущерб	Упущенная выгода
Расходы на расследование и локализацию инцидента	Прибыль от клиентов, расторгнувших договоры после кибератаки и/или не подписавших договоры по ее причине
Компенсация сверхурочных для работников оператора, привлеченных на экстренное устранение последствий инцидента	Отток клиентов/заказов, вызванный блокировкой информационных систем
Расходы на закупку нового оборудования взамен поврежденного вренодосами, а также на услуги по их установке. Расходы на восстановление заблокированной или утраченной информации	

Мировой опыт указывает, что основная часть убытков от кибератак выражается **в упущенной выгоде**. Показательные примеры – это убытки SK Telecom (Южная Корея, утечка данных) и JLR (Великобритания, ransomware). В России общество менее активно реагирует на кибер-инциденты и утечки, что уменьшает возможные размеры убытков. Размеры штрафов за утечку персональных данных и нарушение требований к кибербезопасности также меньше аналогичных за рубежом.



Примеры в РФ: убытки «Аэрофлота» от кибератаки в июле 2025 были оценены экспертами в 275 млн. руб. Основная причина – простой авиационного парка. Аналогичный простой сети магазинов «ВинЛаб» оценивают в диапазоне от 0,8 до 1,2 млрд. руб.



В обоих случаях основную сумму убытков **составила упущенная выгода** – доходы, которые бизнес извлек бы в обычных условиях деятельности, но не получил из-за нарушения своих прав (ст. 15 ГК РФ)

Case Study: реальный ущерб

Реальный ущерб – это расходы на восстановление нарушенного права, утрата или повреждение имущества (ч. 2 ст. 15 ГК РФ)

Реальный ущерб возникает у цели кибертаки. При этом он может взыскать такой ущерб с лица (*например, подрядчика*), чья халатность привела к появлению возможности для реализации кибератаки

А72-10511/2024 *Решение АС Ульяновской области от 25.08.2025*

Заказчик купил серверное оборудование и для его установки и переноса ИТ-систем на новый сервер приобрел услуги Исполнителя. В ходе выполнения работ что-то пошло не так и Исполнитель, для упрощения своей работы, установил на всех рабочих станциях (компьютерах) слабые пароли – 123456. Более того, всем станциям он дал права администратора. После этого одна из станций была взломана, и, пользуясь правами админа, вся сеть была заражена вирусом-шифровальщиком.

Хотя кибератака и была совершена третьим лицом, некачественное оказание услуг Исполнителем создало почву для ее успешной реализации. Суд указал, что между кибератакой и некачественным исполнением услуг есть прямая причинно-следственная связь. Он обязал Исполнителя компенсировать убытки Заказчика на восстановление инфраструктуры, но не посчитал, что Исполнитель должен выплатить Заказчику сумму упущенной выгоды.

«…*установлена совокупность элементов для привлечения ИП Цветкова Е.С. к ответственности в виде возмещения реального ущерба, в том числе виновные действия ответчика, выразившиеся в ненадлежащим качестве оказания услуг по установке сервера и переноса базы данных, в результате которых произошла зашифровка и утеря базы данных истца из-за хакерской атаки , причинную связь между данными действиями и возникшим ущербом, а также размер убытков*»

#вирус-шифровальщик #ransomware

NB *Основанием для взыскания убытков послужила причинно-следственная связь между действиями подрядчика и убытками заказчика и общие положения ГК РФ о договорах и ответственности, а не условия договора между сторонами.*

Структура реального ущерба

Суд взыскал с Исполнителя убытки, непосредственно связанные с восстановлением инфраструктуры. К реальному ущербу Суд отнес: 1) расходы на выплату заработной платы сотрудникам за сверхурочную работу, 2) расходы на проведение аудита ИТ-систем и 3) расходы на восстановление ИТ-инфраструктуры

А72-10511/2024 *Решение АС Ульяновской области (стр. 13)*

«…целью данного договора (на оказание услуг по ИБ-консультированию) было не дополнительное расследование причин атаки, а приведение ИТ инфраструктуры к безопасному состоянию»

При этом **расходы на обеспечение кибербезопасности** считаются реальным ущербом только в том случае, если их цель состоит в **восстановлении** инфраструктуры в безопасном состоянии. Дальнейшее повышение безопасности после инцидента – **не убытки**, а добровольное решение, инвестиция владельца инфраструктуры

Case Study: упущенная выгода

Если реальный ущерб обычно возникает у цели атаки, то вот упущенная выгода может возникнуть как у него, так и у его контрагентов. Она как бы расходится волной по цепочке поставок и впоследствии может быть взыскана с первичной цели кибератаки в суде

Что считается упущенной выгодой?

А72-10511/2024 *Решение АС Ульяновской области от 25.08.2025*

В деле, обстоятельства которого описаны на предыдущей странице, Заказчик пытался взыскать упущенную выгоду. Она выражалась в том, что утраченная после кибератаки информация использовалась в бизнесе. **Суд отказал**, поскольку посчитал, что между утратой информации в цифровом виде и снижением прибыли нет **непосредственной логической связи**, а также что точный размер упущенной прибыли не доказан.

«*При этом истец не доказал, что утеря базы данных и время на ее восстановление в результате хакерской атаки, явилось единственным препятствием, не позволившим ему получить доход, что все остальные необходимые приготовления для его получения им были сделаны, не подтвердил доходы, которые он мог и должен был получить, и только действия ответчика стали единственной причиной, лишившей его возможности получить прибыль от невозможности осуществления предпринимательской деятельности*»

#вирус-шифровальщик #ransomware

Существование двух фактов: наличия кибератаки и снижения прибыли после нее для суда **не образуют прямой логической связи**. Необходимо доказать, что последствия кибератаки были единственной причиной снижения прибыли, более того, что кибератака сделала невозможным получение прибыли от реализации конкретной услуги или товара конкретным способом. К примеру в описанном ниже деле Суд посчитал, что у Истца были альтернативные способы реализации услуги (*вместо сайта – телефон и группа в ВК*).

А56-85885/2024 *Постановление 13ААС от 27.10.2025 (в Кассации)*

Обстоятельства дела рассмотрены на стр.12. После кибератаки на ресурсы Провайдера хостинга сайт Заказчика был заблокирован. Следовательно, клиенты Заказчика не могли покупать услуги через сайт (*проводить бронирование санаториев*). Заказчик посчитал это упущенной выгодой и подал иск о ее компенсации Провайдером. **Суд отказал**.

«*...из материалов дела не следует, что в результате произошедшего 19.04.2023 сбоя и отсутствия у потенциальных приобретателей доступа к сайту «сайт-истца.рф» у Общества снизились либо полностью отсутствовали продажи путевок в санатории, что повлекло возникновение упущенной выгоды в заявленном Обществом размере, в том числе, с учетом того, что согласно сообщению, размещенному Обществом на сайте по электронному адресу: https://vk.com/sanatoriirussia, а также сведениям, размещенным на сайте «сайтистца.рф», бронирование также было возможно путем звонка на горячую линию по номеру телефона 8(800)__-__-__ и иными способами*»

#DDoS #кибердиверсия

При подсчете упущенной выгоды стоит использовать совокупность параметров: не только общее снижение прибыли, но и, к примеру, статистику обращений, клиентские пути. Не лишним будет привлечь эксперта и получить его заключение.

Ущерб в облаках

Хостинг и облачные услуги имеют свою специфику – ресурсы одного лица размещаются на мощностях другого. Возникает вопрос: если инфраструктура провайдера подвергается атаке и сбою, то…

кто несет риск сбоя сайта – провайдер или владелец?

В услугах хостинга кибератаки рассматриваются не как внешнее событие, а как **известный и прогнозируемый риск**, который стороны могут самостоятельно распределить в договоре

А40-293189/2022 *Решение АСГМ от 30.03.2023*

Заказчик купил у Исполнителя услуги по хостингу web-сайта и созданию систем его безопасности в облаке. После кибератаки на инфраструктуру Исполнителя все данные были уничтожены полностью. Заказчик обратился в суд с требованием о компенсации ущерба.

Суд указал, что причинно-следственная связь между (не)исполнением условий договора Исполнителем и убытками заказчика отсутствует. Да, Исполнитель был обязан обеспечить безопасность сайта, но строго предусмотренными договором способами. Он не был обязан защищать информацию от полного уничтожения, все остальные требование по безопасности сайта он выполнил. Более того, Провайдер (Исполнитель) принял все разумные меры по восстановлению работы сайта.

«*Исходя из условий заключенного договора следует, что ответчик не брал на себя обязательства обеспечить сохранность сайта истца от любых хакерских угроз, а обязался выполнить установленный перечень работ. В данном случае причиной уничтожения сайта явилась соответствующая хакерская атака, что свидетельствует об отсутствии прямой причинно-следственной связи, поскольку в данном случае причиной возникновения убытков явились противоправные действия неустановленных лиц, а не действия ответчика*»

#DDoS #отказ_системы #кибердиверсия

А56-85885/2024 *Постановление 13ААС от 27.10.2025 (в Кассации)*

Заказчик купил у Исполнителя услугу хостинга своего web-сайта. Инфраструктура Исполнителя (Провайдера) подверглась кибератаки, из-за чего работа сайта Заказчика была приостановлена. Заказчик понес убытки.

Суд посчитал, что Исполнитель принял разумные меры по устранению вреда, в первую очередь, поднял резервную копию сайта и оповестил Заказчика о сбоях. Также Суд обратил внимание на то, что Заказчик не покупал у Исполнителя услуг по обеспечению безопасности web-сайта. Суд отказал Заказчику во взыскании оыбктво с Исполнителя.

#DDoS #отказ_системы

Вывод:

В услугах хостинга и облака кибербезопасность может быть элементом услуг и/или критерием их качества. Следовательно, риск кибератаки **можно и нужно распределять в договоре между Заказчиком и Провайдером**. При этом возможно разделение как по методам защиты, так и по типам последствий

Если же договор между сторонами не содержит условий о распределении риска кибератак, Суды придерживаются позиции, что услуга провайдера хостинга предоставляется «**как есть**». Риск на стороне Заказчика

Итоги: ущерб

Взыскание ущерба от кибератаки в текущей практике представляется достаточно перспективным. Тем не менее, оператор должен подходить к подсчету их размеров и доказыванию достаточно ответственно

Взыскание реального ущерба

Подсчитать и взыскать реальный ущерб проще, чем упущенную выгоду. Основное ограничение в его подсчете – к реальному ущербу относятся только те траты, которые направлены на восстановление системы в формате «как было». Этот же довод является основным в оспаривании размера реального ущерба

Предмет доказывания и доказательства:	1) **Наличие и размер убытков**. Доказательства: первичная документация (договоры и подтверждения платежей). *Содержание договора должно подтверждать, что он направлен на восстановление ущерба*
2) Факт противоправного деяния	3) **Причинно-следственная связь** между деянием и убытками. Доказательства: (совместно с п. 2) переписка между сторонами, журнал посещений, регистрация действий в системах, заключение эксперта, материалы технического расследования

Мы скептически относимся к возможности взыскания суммы выкупа хакерам-вымогателям ввиду незаконного характера такой выплаты…

Взыскание упущенной выгоды

П. 3 ПП ВС от 24.03.2016 №7 указывает, что при доказывании упущенной выгоды учитываются предпринятые меры и действия, направленные на ее получение. При этом необходимо доказать, что организация пыталась получить прибыль альтернативными путями после кибер-инцидента *(а не сложила лапки и ждала компенсации)*

Предмет доказывания и доказательства:	1) **Факт противоправного поведения стороны**. Доказательства: договоры и соглашения между сторонами, информация о кибер-инциденте, записи систем и материалы экспертизы

2) **Реальность возможности получить доход**. Доказательства: клиентский путь, статистика систем и описание их использования в бизнесе, статистика обращений клиентов с использованием системы, затраты на реализацию бизнес-процесса определенным образом

3) **Размер недополученного дохода**. Доказательства: сравнение между обычными показателями конкретных путей, подвергшихся последствиям кибератаки, и их значениями за период восстановления

4) **Причинно-следственная связь** между недополученным доходом и противоправным поведением.

Кибератаки и утечки ПДн

Краткий обзор показательных дел:
А40-199062/2025: намеренные действия сотрудника по преодолению систем защиты не исключают вины Оператора
А39-7047/2025: кибератака не исключает вины Оператора
А55-36038/2025: отсутствие разумных средств защиты свидетельствует о вине Оператора
А40-294681/2025: кибератака не является основание для уменьшения штрафа
А32-60809/2025: Оператор обязан контролировать нелегитимные действия сотрудников
А27-27136/2025: отсутствие ИБ - бездействие

За 2025 год в **9 делах** Оператор сослался на кибератаку, как причину утечки

Ни в одном деле Суд **не признал** кибератаку обстоятельством, исключающим ответственность

При этом Операторы не строили линию защиты на сопоставлении метода кибератаки и своих конкретных действиях по защите данных. Мы считаем, что, не смотря на текущую практику, **кибератаку все еще можно признать обстоятельством, исключающим ответственность по ст. 13.11 КоАП**

Case Study:

В деле, описанном ниже, Оператор вне всяких сомнений доказал наличие кибератаки. И тем не менее, Суд признал его виновным в утечке

А39-7047/2025 *Решение АС Республики Мордовия от 19.12.2025*

Учетная запись подрядчика Оператора была скомпрометирована, в результате чего иностранные хакеры получили доступ к информации на его серверах и скопировали небольшую кадровую базу данных (8 анкет соискателей). Оператор отчитался об утечке в РКН. Суд посчитал, что оператор не доказал, что предпринял всех возможный мер для противодействия кибератаке. Итог: установлена вина Оператора в форме бездействия, но, ввиду совершения нарушения впервые, Суд вынес **предупреждение**

«Доказательства наличия объективных причин, препятствующих соблюдению Оператором требований законодательства, а также свидетельствующие о том, что оно приняло все зависящие от него меры по недопущению совершения правонарушения, в материалы дела не представлены»

#supply_chain #компрометация_УЗ

Причина – Оператор не доказал, что он принял все возможные меры, чтобы остановить кибератаку. Но, если в гражданских спорах Суды исследуют поведение оператора после кибератаки, то в административных делах изучаются действия оператора по заблаговременному предупреждению атак

Подтверждает вывод пояснение, которое Суд дал **малозначительности правонарушения** (ст. 2.9 КоАП) в сфере защиты персональных данных: угроза охраняемым общественным отношениям проявляется не в угрозе субъектам, а в пренебрежении Оператора публично-правовыми **обязанностями по защите** персональных данных

Case Study: 13.11 КоАП в 2023

Начнем с ретроспективы. В 2023 году появилось два дела, в которых суд указал, что кибератака исключает вину Оператора в утечке персональных данных

Упрощая, позиция судов по этим делам звучала так: *не твои действия были формальной причиной утечки, не тебе и отвечать*

05-1048/244/2023 (АльфаСтрахование)
Постановление Мирового судьи судебного участка №244 г. Москвы от 25.09.2023

В результате кибератаки данные были скопированы с серверов Оператора и опубликованы в Интернете. Суд указал, что оператор сделал все возможное, чтобы защитить данные и минимизировать последствия утечки. Итог: дело прекращено ввиду **отсутствия состава** административного правонарушения.

«*...требования, предусмотренные ФЗ №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, выполнены Оператором своевременно и в полном объеме. По сути Оператору вменяется неправомерная передача персональных данных неопределённому кругу лиц, однако виновные в том действия (бездействия) Оператора судом не установлены*»

05-1048/244/2023 (Спортмастер)
Постановление Мирового судьи судебного участка №52 г. Москвы от 05.06.2023

Некие третьи лица получили доступ к учетной записи подрядчика Оператора, обсуживающего его ИТ-системы. Используя привилегированный доступ пподрядчика, они скопировали базы персональных данных Оператора. Роскомнадзор посчитал, что оператор несет ответственность за такую утечку. Суд не согласился: фактическая вина лежит на хакерах, а Оператор сделал все возможное, чтобы предотвратить утечку и минимизировать ее последствия. Дело было прекращено ввиду **отсутствия состава** административного правонарушения.

#supply_chain

Сейчас же Суды смотрят на причину утечки ПДн шире и включают в нее действия по обеспечению ИБ. Тем не менее, эти два дела сформировали перечень действий Оператора после инцидента, которые безотносительно установления вины **помогут уменьшить размер штрафа** по ст. 13.11 КоАП:

Сразу после:	Определить тип атаки, пораженные системы и скомпрометированные учетные записи. Немедленно локализовать инцидент, сбросить пароли пользователей
Собрать доказательства о факте кибератаки, в том числе: докладные записки, данные SEIM/SOC/DLP (в зависимости от типа), журналы регистрации событий учетных записей	**Уведомить РКН** в сроки, установленные ч. 3 ст. 21 ФЗ №152-ФЗ
Далее:	Обратиться в МВД с сообщением о преступлении, предусмотренном ст. 272 (возможно и 272.1) УК РФ
Восстановить защищенность ИТ систем, в том числе с привлечением консультантов	Организовать работу с субъектами персональных данных, направить им рекомендации по смене паролей и установке 2FA, опубликовать пресс-релиз

Case Study: 13.11 КоАП в 2025

Сейчас Суды рассматривают успешную кибератаку, как **возможное доказательство бездействия** Оператора в вопросе обеспечения безопасности данных

А40-294681/2025 *Решение АСГМ от 24.12.2025*

В результате кибератаки кадровая база данных Оператора попала в открытый доступ. Суд решил, что Оператор не принял должных мер по обеспечению безопасности

«...у Оператора имелась возможность для соблюдения правил и норм, за нарушение которых ч. 1 ст. 13.11 КоАП РФ предусмотрена административная ответственность, но им не были приняты все зависящие от него меры по их соблюдению. Доказательств, свидетельствующих о невозможности исполнить установленную законодательством обязанность по соблюдению требований законодательства Оператором не представлено»

#компрометация_УЗ

Суды допускают ссылку на кибератаку, как на чрезвычайное обстоятельство, но только если Оператор **дополнительно** докажет, что сделал все возможное, чтобы ей противодействовать

А27-27136/2025 *Решение АС Кемеровской области от 19.01.2025*

Хакеры разместили данные из 1С-систем Оператора в публичном доступе. Оператор доказал факт кибератаки, но суд посчитал его виновным в утечке – должны уровень информационной безопасности обеспечен не был

«Доказательств невозможности соблюдения обществом указанных требований, в силу чрезвычайных событий и обстоятельств, которые оно не могло предвидеть и предотвратить при соблюдении той степени заботливости и осмотрительности, которая от него требовалась, в материалах дела не имеется...»

Но критериев или перечня «*всех возможных мер*» по защите данных в практике на текущий момент нет. Тревожным примером выступает дело А40-36038/2025, в котором атака внутреннего нарушителя была реализована через фотографирование экрана на личный телефон. Технически противодействовать такой атаке крайне затруднительно, и, тем не менее, Суд пришел к выводу о бездействии Оператора

А40-36038/2025 *Решение АСГМ от 19.11.2025**

Бывшие сотрудники Оператора перед увольнением скопировали базы персональных данных Оператора, сфотографировав их на телефон. Суд посчитал, что это утечка, а Оператор виноват в том, что допустил ее

«...На основании изложенного в действиях Оператора выявлено нарушение требований части 1 статьи 6, статьи 7 и статьи 10.1 Закона «О персональных данных» в части предоставления неправомерного доступа к базе данных Оператора, содержащей персональные данные из информационной системы, повлекшего за собой распространение персональных данных неограниченному кругу лиц»

На наш взгляд, текущая практика объясняется инструментализмом в ссылке на кибератаку, как причину утечки – ее пытаются выдать за **индульгенцию** саму по себе. Операторы не доказывали свою добросовестность, ограничиваясь доказыванием недобросовестности хакеров

Стратегия защиты: 13.11 КоАП

Далее мы представим наш личный взгляд на наиболее выигрышную стратегию использования факта кибератаки в защите по ст. 13.11 КоАП. Стратегия основана на доказывании отсутствия вины Оператора в форме бездействия. Лучший результат – прекращение дела ввиду отсутствия состава административного правонарушения. Позиция для отступления – предупреждение со ссылкой на малозначительность

Основа стратегии *– доказывание максимальной добросовестности Оператора в вопросе защиты информации и противодействии утечкам*

Инструментарий *– ссылки на фактические действия оператора по защите информации, их* ***разумность, структурированность*** *и* ***достаточность*** *в условиях несовершенства технических мер противодействия угрозам*

Матрица нормативно-правовых ссылок:

Ст. 3.1. КоАП: целью административного наказания является предупреждение совершения новых правонарушений → *если оператор уже принимает все разумные меры по защите данных, его не к чему мотивировать*

Ч. 2 ст. 2.1. КоАП: юридическое лицо признается виновным только в том случае, если у него имелась возможность для соблюдения требований законодательства → *оператор не несет ответственность, если предпринял все разумные меры по обеспечению ИБ до той степени, что дальнейшее повышение безопасности представляется технически или экономически нецелесообразным*

Ч. 1 ст. 1.5. КоАП: лицо подлежит ответственности только за те правонарушения, в отношении которых установлена его вина

П. 3 ст. 26.1 КоАП: виновность лица правонарушении подлежит установлению (на основании всестороннего изучения обстоятельств дела – ст. 26.11 КоАП

Ч. 2.9. КоАП + п. 21 ПП ВС от 24.03.2005 №5: малозначительность выражается в отсутствии угрозы охраняемым общественным отношениям, что, в теории, позволяет применить малозначительность и к крупной утечке в случае исключительного уровня безопасности у оператора

Указанная стратегия полностью зависит от фактических действий Оператора по защите информации. При этом она требует действий как **до кибератаки**, так и **после** нее

Стратегия защиты: 13.11 КоАП

Если сравнивать решения по делам 2023 и 2025 года, то в их тексте мы найдем одни и те же критерии, по которым суды оценивали обстоятельства дела. Разница лишь в том, что Спортмастер и АльфаСтрахование смогли привести доводы в обоснование своей добросовестности, а операторы по делам 2025 года смогли лишь доказать факт кибератаки

Ниже мы представим свои варианты доказательств и необходимый действий до и после кибератаки

До кибератаки и утечки

1) Подготовка Модели угроз. Если модель угроз Оператора предусматривает реализовавшуюся кибератаку, то он сможет применить ст. 3.1. КоАП, указав, что его системы защиты были готовы к отражению конкретной угрозы и он вел себя разумно в вопросе защиты персональных данных

2) Доказательства факта защиты информации. Основу здесь составляют приказы о вводе систем в эксплуатацию и данные этих систем, фиксирующие инцидент. Дополнительным доказательством выступят регулярные профильные мероприятия: аудиты, тренировки, до-установка СЗИ. Это позволит применить ч. 2 ст. 2.1. КоАП

Наличие доказательств подготовки к отражению конкретного типа кибератак позволят Оператору представить кибератаку не как неожиданное действие некий злых третьих лиц (это проигрышная тактика), а как предусмотренным оператором риск. Причиной же успеха кибератаки будет не бездействие оператора, а намеренное преодоление третьими лицами всех разумных способов защитить данные

После утечки

Если подготовка к возможной атаке говорит о должной осмотрительность оператора, то реагирование на инцидент указывает на его полную добросовестность. Ниже наиболее важные по нашему мнению действия:

Локализация утечки и минимизация ее последствий

Сообщение в РКН и предоставление результатов внутреннего расследования

Минимизация последствий утечки для субъекта, его уведомление и предоставление информации о способах повышения безопасности на его стороне

О реагировании на утечку есть отдельный материал в нашем telegram-канале

project101

§ Бумажная безопасность

Мы считаем, что текущая практика судов подчеркивает значение юридического элемента обеспечения безопасности. Ему отводится особая роль в логике доказывания добросовестности организации. Под юридическим элементом и бумажной безопасностью мы пониманием разработку локальных нормативных актов и документов в сфере ИБ

Бумажная безопасность:

Модель угроз позволяет перевести линию защиты из *«мы не знали, мы были не готовы, смилуйтесь»* в *«мы вели себя разумно, готовились и сделали все возможное». Такая позиция имеет бóльшие шансы на успех и в административном, и в гражданском процессе*

Акт оценки уровня защищенности / заключение аудита позволит уменьшить сомнения суда в разумности и достаточности мер, принятых оператором для предотвращения угрозы

Перечень систем защиты информации или иной документ, который бы отвечал на вопрос «*а как вы противодействуете угрозе №__?*». В случае, если инцидент будет реализован способом, предусмотренным Моделью угроз, оператору необходимо предоставить доказательства превентивных действий по ее предотвращению. Такое доказательство позволит перевести риторику из вопроса неосмотрительности оператора в вопрос пределов эффективности методов и систем защиты информации. Суды понимают, что всё и от всего защитить нельзя

Кризисные планы и **должностные инструкции** должны устанавливать право и порядок перевода бизнеса в кризисный режим работы с контрагентами. В первую очередь – защищать человека, который решил действовать, а не ждать разблокировки систем, и давать ему возможность так действовать