Исследование судебной практики по уголовным делам, связанным с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну, 2019-2021 гг.

Оглавление

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch подготовил отчет по итогам исследования судебной практики по делам, связанным с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну (статья 183 УК РФ).

В рамках исследования изучены решения судов первой инстанции, вынесенные в 2019-2021 годах. В отчете сделаны выводы о типах решений, приведены доли видов наказаний по приговорам, даны размеры судебных штрафов в результате прекращения уголовных дел на основании статьи 25.1 УПК РФ. Также авторы приводят результаты исследования каналов утечек информации, относящейся к категории «коммерческая тайна».

Авторы отмечают, что исследование не опирается на какие статистические сведения и не претендует на полноту информации, но позволяет выявить основные тенденции в судебной практике по статье 183 УК РФ, определить размер наказаний, выявить отраслевую принадлежность пострадавших компаний и организаций, представить основные каналы утечки.

Только факты

- По делам, связанным с незаконным получением и разглашением коммерческой, банковской и налоговой тайны, в 2019-2021 гг. было осуждено 117 человек.
- Всего за три года было рассмотрено 188 дел по различным частям статьи 183 УК РФ.
- Более 63% рассмотренных дел и более 65% осужденных лиц приходятся на часть 3 статьи 183 УК РФ.
- Более 46% рассмотренных дел по статье 183 УК РФ имели дополнительную квалификацию по одной или нескольким статьям (272 УК РФ, 138 УК РФ и др.).
- По итогам рассмотрения 44,3% дел по статье 183 УК РФ судьи выносили обвинительные приговоры, почти 40% дел было прекращено.
- 44,7% осужденных приговаривались к штрафам, 36,9% получили условные сроки, 9,2% - реальные сроки, 9,2% - исправительные работы.
- 2 года тюремного заключения – самое строгое наказание по статье 183 УК РФ, назначенное в период 2019-2021 гг.
- 1 миллион рублей – самый крупный штраф, назначенный осужденному по статье 183 УК РФ в период 2019-2021 гг.
- Несмотря на прекращение 75 уголовных дел (около 40% от всех рассмотренных), в 25 подобных случаях были назначены судебные штрафы.
- Примерно в 75% рассмотренных случаев конфиденциальная информация была скомпрометирована через Сеть или сервисы мгновенных сообщений.
- Более 80% пострадавших организаций – это финансовые компании и операторы связи.
- Порядка 70% подсудимых были непривилегированными сотрудниками, 18% - внешними нарушителями, более 10% - руководителями разного уровня.

Сокращения

ГАС «Правосудие»	Государственная Автоматизированная система Российской Федерации «Правосудие»
ПДн	Персональные данные
СК	Следственный комитет Российской Федерации
УК РФ	Уголовный Кодекс Российской Федерации
УПК РФ	Уголовно-процессуальный кодекс Российской Федерации
ЭАЦ	Экспертно-аналитический центр ГК InfoWatch

Подход и предмет исследования

Цель исследования – выявление основных закономерностей (тенденций) судебной практики по отобранным для исследования уголовным делам, в частности, определение типов наказаний, их строгости, категорий виновных лиц, отраслевой принадлежности пострадавших компаний, выяснение каналов утечки информации и т.д.

Для этого исследования мы выбрали статью 183, входящую в **Главу 22 УК РФ «Преступления в сфере экономической деятельности»:**

Таблица 1. Статья 183 УК: суть по частям и наказания

	Название
Статья УК РФ 183	**Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайны**
	Ч.1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, обмана, шантажа, принуждения, подкупа или угроз, а равно иным незаконным способом - (в ред. Федерального закона от 11.06.2021 N 216-ФЗ) наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок. (в ред. Федеральных законов от 07.12.2011 N 420-ФЗ, от 29.06.2015 N 193-ФЗ)
	Ч.2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, - наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок. (в ред. Федеральных законов от 07.12.2011 N 420-ФЗ, от 29.06.2015 N 193-ФЗ, от 11.06.2021 N 216-ФЗ)
	Ч.3. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности. (в ред. Федерального закона от 11.06.2021 N 216-ФЗ) наказываются штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок. (в ред. Федеральных законов от 07.12.2011 N 420-ФЗ, от 29.06.2015 N 193-ФЗ)
	Ч.4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, - наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет. (в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

В соответствии со статьей 183 УК РФ, предусматривается уголовная ответственность за совершение двух разных деяний. Первое – собирание сведений, которые составляют коммерческую, налоговую или банковскую тайну. Второе - незаконное разглашение или использование сведений, составляющих такую тайну. Таким образом, эти деяния объединяет общий предмет посягательства – сведения, составляющие коммерческую, налоговую или банковскую тайну.

Исследуемый период

По статье 183 УК РФ были выбраны дела, рассмотренные судами первой инстанции в 2019-2021 гг., то есть за трехлетний период.

База судебных дел

Для исследования составлен список судебных дел по выбранной для исследования статье УК РФ на основе данных **Государственной Автоматизированной системы Российской Федерации «Правосудие» (ГАС «Правосудие»)**.

Для конкретизации деталей судебных дел использованы сайты судов общей юрисдикции.

В базу судебных дел внесены данные о судебных делах за 2019-2021 гг. по выбранной статье, включая:

- Номер дела
- Описание сути нарушения
- Дата поступления дела
- Дата судебного решения
- Регион
- Уровень и тип суда
- ФИО ответчика
- Пострадавшая компания (организация)
- Тип решения
- Тип и размер наказания
- Каналы передачи информации

Примечание. Часть записей в ГАС «Правосудие» не содержит судебные акты, также зачастую скрыта информация по участникам судебного процесса, поэтому установить и проанализировать суть всех рассматриваемых дел невозможно.

Подследственность

Согласно подследственности, установленной частью 2 статьи 151 Уголовно-процессуального кодекса Российской Федерации (УПК РФ), предварительное следствие по уголовным делам о преступлениях, предусмотренных статьей 183 УК РФ, проводится следователями органов внутренних дел Российской Федерации. Предварительное следствие может проводиться также следователями органа, выявившего эти преступления.

Официальная статистика

Судебный департамент

В статистических сведениях, опубликованных на сайте Судебного департамента при Верховном Суде Российской Федерации, есть отдельные отчеты о количестве лиц, привлеченных к уголовной ответственности.

Согласно данным Судебного департамента, всего по статье 183 УК РФ осуждено:

- в 2019 году – 41 человек, из них 2 человека по ч.1, 7 человек - по ч.2, 32 человека по ч.3, 0 человек - по ч.4;
- в 2020 году – 35 человек, из них 3 человека по ч.1, 10 человек по ч.2, 22 человека по ч.3, 0 человек - по ч.4;
- в 2021 году – 41 человек, из них 3 человека - по ч.1, 15 человек - по ч.2, 23 человека- по ч.3, 0 человек - по ч.4.

Таблица 1. Количество лиц, осужденных по статье 183 УК РФ в 2019-2021 гг.

2019	Части статей			Всего осуждено по статье 183 УК РФ
Статья 183 УК РФ	137 часть 1	137 часть 2	137 часть 3	
Количество дел	**2**	**7**	**32**	**41**
2020	Части статей			Всего осуждено по статье 183 УК РФ
Статья 183 УК РФ	137 часть 1	137 часть 2	137 часть 3	
Количество дел	**3**	**10**	**22**	**35**
2021	Части статей			Всего дел по статье 183 УК РФ
Статья 183 УК РФ	137 часть 1	137 часть 2	137 часть 3	
Количество дел	**3**	**15**	**23**	**41**

Источник: Судебный департамент при Верховном Суде РФ.

Таким образом, всего за три года по статье 138 УК РФ было осуждено 117 человек. Количество осужденных по каждой части статьи 183 УК РФ за три года представлено на Рисунке 1.

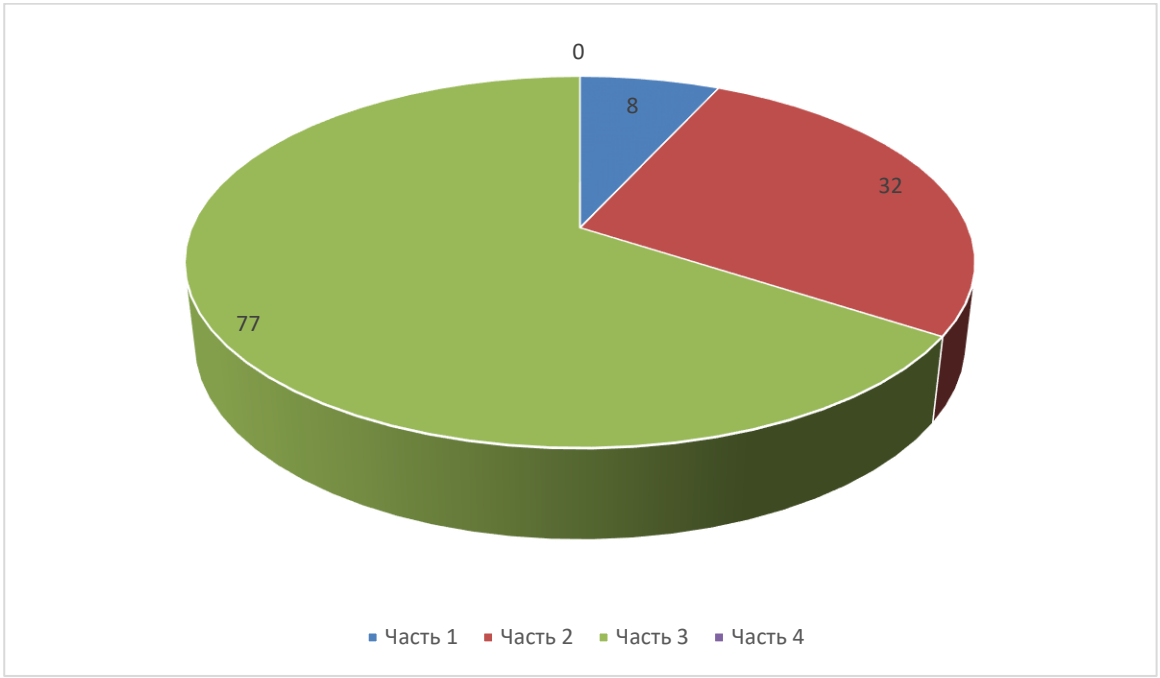

Рисунок 1. Количество осужденных по разным частям ст. 183 УК РФ, 2019-2021 гг.

Данные о количестве возбуждённых и завершенных уголовных дел по статье 183 УК РФ отсутствуют, имеется статистика только по главе 22 УК РФ в целом (статьи 169 - 200.6).

МВД России

Министерство внутренних дел в публикациях не выделяло преступления по статье 183 УК РФ в совокупности зарегистрированных преступлений экономической направленности.

Сведения в ГАС РФ «Правосудие»

Обратившись к государственной автоматизированной системе «Правосудие» для уточнения количества дел, наличия актов судебных дел по указанным статьям в целях их исследования по сути нарушений и по другим данным, мы получили следующие результаты по статье 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайны»:

- за 2019 год обнаружено 69 записей о делах, рассмотренных в судах первой инстанции;
- за 2020 год обнаружено 79 записей о делах, рассмотренных в судах первой инстанции;
- за 2021 обнаружено 40 записей о делах, рассмотренных в судах первой инстанции.

Вероятно, в ГАС РФ «Правосудие» ко времени исследования (май-июнь 2022 г.) не были внесены все дела, рассмотренные в 2021 г.

Таблица 2. Количество дел по статье 183 УК РФ, рассмотренных судами первой инстанции в 2019-2021 гг.

2019	Части статей			Всего дел по статье 183 УК РФ
Статья 183 УК РФ	137 часть 1	137 часть 2	137 часть 3	
Количество дел	**13**	**11**	**45**	**69**
2020	Части статей			Всего дел по статье 183 УК РФ
Статья 183 УК РФ	137 часть 1	137 часть 2	137 часть 3	
Количество дел	**12**	**19**	**48**	**79**
2021	Части статей			Всего дел по статье 183 УК РФ
Статья 183 УК РФ	137 часть 1	137 часть 2	137 часть 3	
Количество дел	**7**	**7**	**26**	**40**

Источник: ГАС «Правосудие»

Согласно сведениям из ГАС «Правосудие», всего за три года судами первой инстанции было рассмотрено 188 дел по статье 183 УК РФ.

Таким образом, в 2019 г. 18,8% дел рассмотрены по части 1, 15,9% дел – по части 2, 65,3% дел – по части 3.

В 2020 г. 15,2% дел рассмотрены по части 1, 24% - по части 2, 60,8% - по части 3.

В 2021 г. соотношение было следующее: по 17,5% дел пришлись на части 1 и 2, 65% дел – на часть 3.

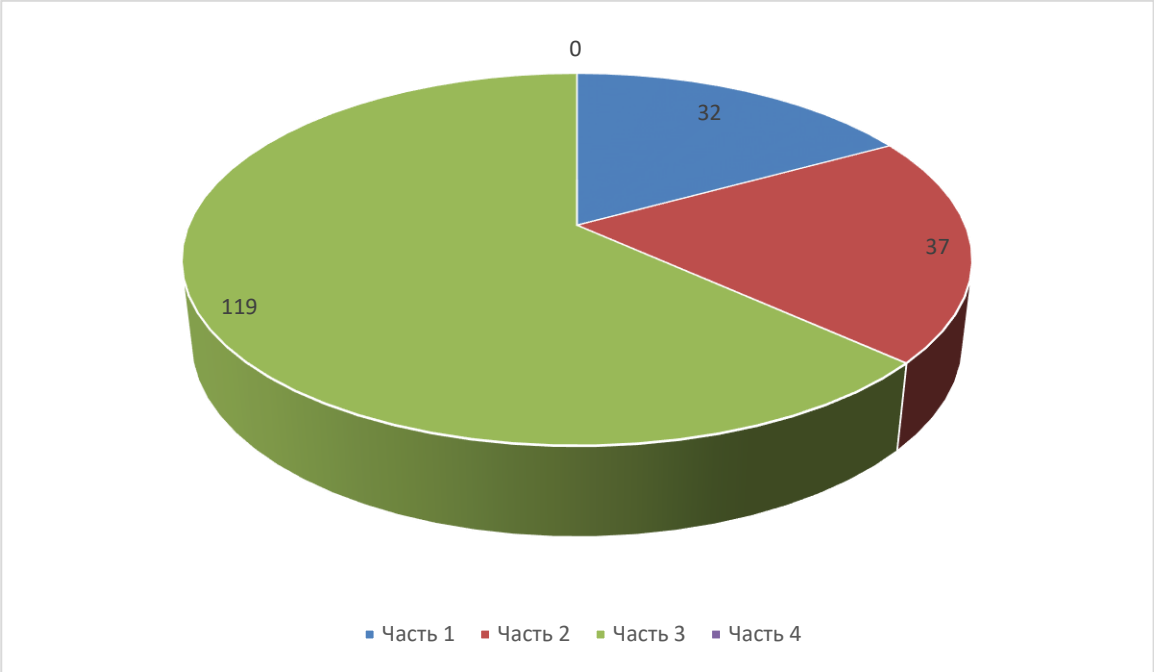

Рисунок 2. Количество дел, рассмотренных по разным частям ст. 183 УК РФ, 2019-2021 гг.

В 2019-2021 гг. более 63% дел по статье 183 УК РФ рассматривались в части 3 этой статьи.

Из всех вошедших в поле исследования дел 86,8% рассмотрены городскими, районными и межрайонными судами, 5,8% - областными, краевыми и республиканскими, 6,9% - мировыми, 0,5% - военными.

Результаты исследования

Из выбранных в ГАС РФ «Правосудие» записей по статье 183 УК РФ большинство рассмотренных судами первой инстанции дел – 53,7%, затрагивали только одну эту статью. Еще 46,3% дел были сопряжены с обвинениями как по 183 статье УК РФ, так и по другим статьям, то есть имели дополнительную квалификацию. Чаще всего обвиняемые по статье 183 УК РФ также обвинялись по статье 272 УК РФ «Неправомерный доступ к компьютерной информации» (в подавляющем большинстве случаев обвинение выдвигалось по части 3 – «Деяния, предусмотренные частями первой и второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой лиц либо лицом с использованием своего служебного положения»).

В целом за период 2019-2021 гг. по итогам рассмотрения выбранных дел суды в 44,3% дел выносили обвинительные приговоры, в 39,9% случаев дела были прекращены (по ходатайству следователей, в связи с примирением сторон и т.д.). В 1,1% случаев вынесены оправдательные приговоры, в 1,6% принимались решения о возвращении дел следствию. Распределение по типам судебных решений по статье 183 УК РФ в судах первой инстанции приведено на Рисунке 3.

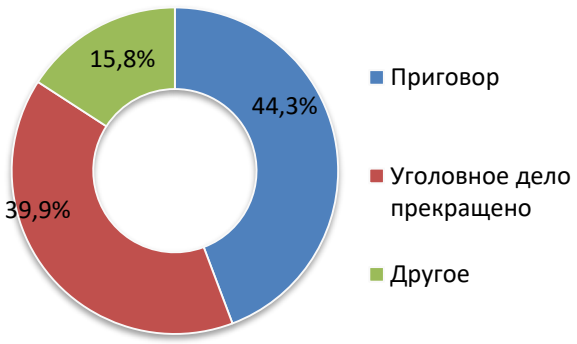

Рисунок 3. Типы решений в результате рассмотрения дел по ст. 183 УК РФ, 2019-2021 гг.

Наиболее частые деяния, по которым рассматриваются дела по статье 183 УК РФ, – разглашение и намеренная передача менеджерами операторов связи информации абонентов (персональные данные, детализация вызовов), а также передача банковскими служащими сведений, относящихся к категории «банковская тайна» (информация о счетах и картах клиентов финансовых организаций).

Адин А.П. подозревается в том, что в период с 04.05.2018 по 02.08.2018, являясь <данные изъяты> группы офисов № <данные изъяты> на основании приказа (распоряжения) о приеме на работу № 5684-к от 04.05.2018, находясь в офисе указанной организации, расположенном в г. Нижний Тагил, ул. <данные изъяты>, имея умысел на незаконные получение и разглашение сведений, составляющих коммерческую тайну, без согласия их владельца, в нарушение должностной инструкции специалиста офиса, умышленно, из корыстных побуждений, используя свое служебное положение, загружал на рабочий стол персонального компьютера посредством своей учетной записи детализации телефонных переговоров абонентов «<данные изъяты>», которые впоследствии реализовывал неустановленному в ходе предварительного следствия лицу посредством кроссплатформенного мессенджера «<данные изъяты>» за денежное вознаграждение, тем самым незаконно использовал сведения, составляющие коммерческую тайну «<данные изъяты>».

Действия Адина А.П. квалифицированы следователем по ч. 3 ст. 183 УК РФ как незаконные собирание и использование сведений, составляющих коммерческую тайну, без согласия их владельца лицом, которому она была доверена по работе, совершенное из корыстной заинтересованности.

Шачнев Д.Г. умышленно, из личной заинтересованности, незаконно, отправил, то есть фактически скопировал, на свой личный электронный почтовый ящик ..., где хранил до момента обнаружения его действий службой безопасности КРФ АО «Россельхозбанк», то есть до 28.02.2019 включительно, и тем самым вывел из под контроля КРФ АО «Россельхозбанк», позволяющего обеспечить конфиденциальность сведений, электронные файлы документов АО «Россельхозбанк», содержащих сведения о части кредитных досье клиентов банка, о содержании и результатах предконтрактных переговоров, о содержании заключенных банком договоров (соглашений) и сделок, о содержании банковских гарантий, выданных банком, о содержании распорядительно – нормативных документов банка, логин и пароль, используемые в банке в системах разграничения доступа, а также аналитическую информацию по клиентам, составленную в банке, информацию о методах расчета стоимости услуг банка, о методах оценки кредитоспособности заемщиков банка, о методах оценки имущества, являющегося предметом залога, и внутрибанковскую переписку, то есть документов, содержащих сведения, составляющие коммерческую тайну АО «Россельхозбанк» в соответствии с пунктами 2.4., 3.1., 3.2., 3.6., 5.4., 6.1., 6.2., 6.4., 6.6., 6.7., 6.8. Перечня информации, составляющей коммерческую тайну АО «Россельхозбанк», а также электронные файлы документов АО «Россельхозбанк», содержащих сведения о клиентах АО «Россельхозбанк», которые в соответствии со статьей 857 Гражданского Кодекса РФ и статьей 26 Федерального закона от 02.12.1990 № 395-I «О банках и банковской деятельности» составляют банковскую тайну АО «Россельхозбанк».

Из наказаний для осужденных по статье 183 УК РФ чаще всего встречается штраф – в 44,7% приговоров. Более чем в трети случаев вынесения наказаний судьи назначали условный срок – от 6 месяцев по одной статье, до 4 лет - по совокупности нескольких. (Рисунок 4).

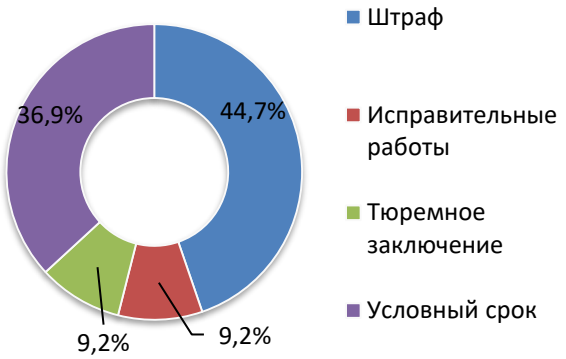

Рисунок 4. Распределение наказаний по ст. 183 УК РФ, 2019-2021 гг.

Самое строгое наказание, назначенное судом по статье 183 УК РФ, - два года тюремного заключения (правда, с отсрочкой до достижения детьми осужденной 14-летнего возраста).

Согласно разработанному плану Федориной., в силу занимаемого служебного положения, имея доступ к автоматизированной системе Банка, содержащей сведения о клиентах, счетах по вкладам клиентов, размере денежных средств (остатках) на этих счетах и иной информации, позволяющей сделать выводы о благонадежности клиента, в соответствии со ст. 26 ФЗ РФ от 02.12.1990 № 395-1 «О банках и банковской деятельности» и ст. 857 ГК РФ от 26.01.1996 № 14-ФЗ являющиеся банковской тайной, об ответственности за конфиденциальность и сохранность которых Федориной письменно предупреждена, воспользовавшись тем, что за ее действиями никто не наблюдает и не контролирует, находясь на своем рабочем месте, намеревалась произвести выборку счетов по вкладам, заключенным на длительный срок, по которым клиентами Банка в течение продолжительного времени не проводились операции и по которым наименее вероятно обращение клиентов, а также, достоверно зная требования ПАО «Сбербанк» к заемщикам, выборку клиентов, имеющих положительную кредитную историю в ПАО «Сбербанк», что гарантировало положительное решение ПАО «Сбербанк» о выдаче кредита выбранному ею клиенту.

<...>

Совершенное Федориной Д. И. деяние в части незаконного использования сведений в отношении ФИО5, составляющих банковскую тайну, суд квалифицирует по ч. 3 ст. 183 УК РФ., а именно как незаконное использование сведений, составляющих банковскую тайну, без согласия их владельца лицом, которому она была доверена по работе, совершенное из корыстной заинтересованности.

Совершенное Федориной Д. И. деяние в части хищения денежных средств ПАО «Сбербанк» в сумме 1 808 698 рублей 14 копеек суд квалифицирует по ч. 4 ст. 159 УК РФ, а именно как мошенничество, то есть хищение чужого имущества путем обмана, совершенное лицом с использованием своего служебного положения, в особо крупном размере.

С учетом дополнительной квалификации состава преступлений (привлечение к ответственности еще по одной или нескольким статьям, помимо 183 УК РФ), максимальный размер наказания составил 7 лет тюрьмы.

Максимальный размер штрафа по статье 183 УК РФ составил 1 млн рублей, минимальный – 8 тыс. рублей. Средний размер штрафа – 123,8 тыс. рублей.

Мухаметов А.Р., в период с <дата изъята> по <дата изъята> являясь ведущим специалистом по обслуживанию частных лиц сектора подменного фонда Управления продаж и обслуживания в сети внутреннего структурного подразделения для физических лиц дополнительного офиса <номер изъят> отделения «<данные изъяты>» <номер изъят> <данные изъяты>, находясь в помещении дополнительного офиса <номер изъят>, расположенного по адресу: <адрес изъят> в период с <дата изъята> по <дата изъята>, являясь руководителем дополнительного офиса <номер изъят> отделения «Банк Татарстан» <номер изъят> <данные изъяты>, находясь в помещении дополнительного офиса <номер изъят>, расположенного по адресу: <адрес изъят>, путем незаконного ознакомления со счетами клиентов <данные изъяты>, с использованием своего рабочего компьютера, а также установленной на нем программы <данные изъяты>, с целью незаконного получения сведений, составляющих банковскую тайну, осуществлял поиск, при помощи присвоенного ему логина и пароля, путем ввода в программу <данные изъяты> информации ФИО клиента, даты рождения, паспортных данных. После чего, получал доступ к информации, составляющей банковскую тайну, а именно полным персональным данным клиента, об открытых на клиента счетах, сведения о состоянии счета клиента, открытых во всех отделениях <данные изъяты> <данные изъяты>, остатках денежных средств на счетах клиента. Далее, Мухаметов А.Р. осуществлял вход в файлы, содержащие сведения о конкретных счетах клиентов, движении денежных средств по указанным расчетным счетам и производил печать реквизитов счета клиента. Таким образом, Мухаметов А.Р. неправомерно, в отсутствии служебной необходимости, а также в отсутствие клиентов, совершил 514 операций по собиранию сведений о счетах 110 клиентов <данные изъяты>, составляющих банковскую тайну.
<…>
Признать Мухаметова А.Р., виновным в совершении преступления, предусмотренного частью 3 статьи 183 УК РФ и назначить ему наказание в виде штрафа в размере 500 000 (пятьсот тысяч) рублей в доход государства, с лишением права занимать должности, связанные с осуществлением банковской деятельности сроком на 2 (два) года 6 (шесть) месяцев.

Более 9% наказаний – это исправительные работы. Осужденные получали от 6 месяцев до 2 лет таких работ.

В соответствии со статьей 25.1 Уголовно-процессуального кодекса РФ, суд по собственной инициативе или по результатам рассмотрения ходатайства, поданного следователем с согласия руководителя следственного органа, либо дознавателем с согласия прокурора, в порядке, установленном настоящим Кодексом, в случаях, предусмотренных статьей 76.2 Уголовного кодекса Российской Федерации, вправе прекратить уголовное дело или уголовное преследование в отношении лица, подозреваемого или обвиняемого в совершении преступления небольшой или средней тяжести, если это лицо возместило ущерб или иным образом загладило причиненный преступлением вред, и назначить данному лицу меру уголовно-правового характера в виде **судебного штрафа**.

В материалах в системе «Правосудие» о вынесенных в 2019-2021 гг. решениях по статье 183 УК РФ найдена информация о случаях назначения 25 судебных штрафов лицам, в отношении которых прекращены уголовные дела. Размер 15 судебных штрафов известен из доступных материалов. Минимальный размер судебного штрафа составил 5 тыс. рублей, максимальный – 300 тыс. рублей. Чаще всего встречались судебные штрафы размерами 50 тыс. и 100 тыс. рублей – по три случая.

Григорьева М.А., занимая должность управляющей по малому и среднему бизнесу операционного офиса «Т» ООО «В» (далее по тексту Банк), расположенного по адресу: <адрес>, находясь на рабочем месте, достоверно зная о том, что банковская тайна - это юридический принцип в законодательстве Российской Федерации, в соответствии с которым банки и иные кредитные организации защищают сведения о вкладах и счетах своих клиентов и корреспондентов, банковских операциях по счетам и сделкам в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни, на основании приказа (распоряжения) о переводе работника на другую работу №л от ДД.ММ.ГГГГ, достоверно зная о том, что согласно п. 6.5 должностной инструкции от ДД.ММ.ГГГГ несет ответственность за разглашение сведений о деятельности Банка и его клиентах, составляющих коммерческую и банковскую тайну, в нарушение положений ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности», в период времени с 01.01.2017 г. по 01.06.2018 г. осуществляла незаконное разглашение сведений, составляющих банковскую тайну, без согласия их владельца в пользу третьих лиц, достоверно зная о том, что указанные сведения стали Григорьевой М.А. известны по работе, которые были совершены Григорьевой М.А. из корыстной заинтересованности.

<…>

В судебном заседании установлено, что Григорьева М.А. обвиняется в совершении преступления, относящегося в соответствии с ч. 3 ст. 15 УК РФ к категории преступлений средней тяжести, ранее не судима (т.14, л.д.30), полностью признала свою вину, в содеянном раскаялась, загладила причиненный преступлением вред путем внесения пожертвования в ГБУЗ ТО «Т» в сумме 50 000 рублей (т.13, л.д.196, 197-198), публично принесла свои извинения потерпевшей стороне (т.13, л.д.213), участковым уполномоченным по месту жительства характеризуется удовлетворительно (т.14, л.д.36), во время работы в АО «В» зарекомендовала себя положительно (т.13, л.д.180), на учете в наркологическом диспансере г. Тюмени не состоит (т.14, л.д.31-32), на учете в психиатрическом диспансере г. Тюмени не состоит (т.14, л.д.33-34), имеет на иждивении <данные изъяты> (т.13, л.д.181-182).

<…>

Ходатайство начальника отделения СЧ СУ УМВД России по г. Тюмени РЕВ. о прекращении уголовного дела в соответствии со ст.25.1 УПК РФ и назначении Григорьевой М.А. меры уголовно-правового характера в виде судебного штрафа, предусмотренной ст. 104.4 УК РФ, удовлетворить.

Прекратить уголовное дело № в отношении Григорьевой М.А., обвиняемой в совершении преступления, предусмотренного ч.3 ст.183 УК РФ, по основанию, предусмотренному ст. 25.1 УПК РФ.

Назначить Григорьевой М.А. меру уголовно-правового характера в виде судебного штрафа в размере 100 000 (сто тысяч) рублей в доход государства, который ей необходимо уплатить не позднее ДД.ММ.ГГГГ.

Самые распространенные каналы компрометации информации, которые использовали лица, осужденные по статье 183 УК РФ, – это мессенджеры и Сеть (Рисунок 5).

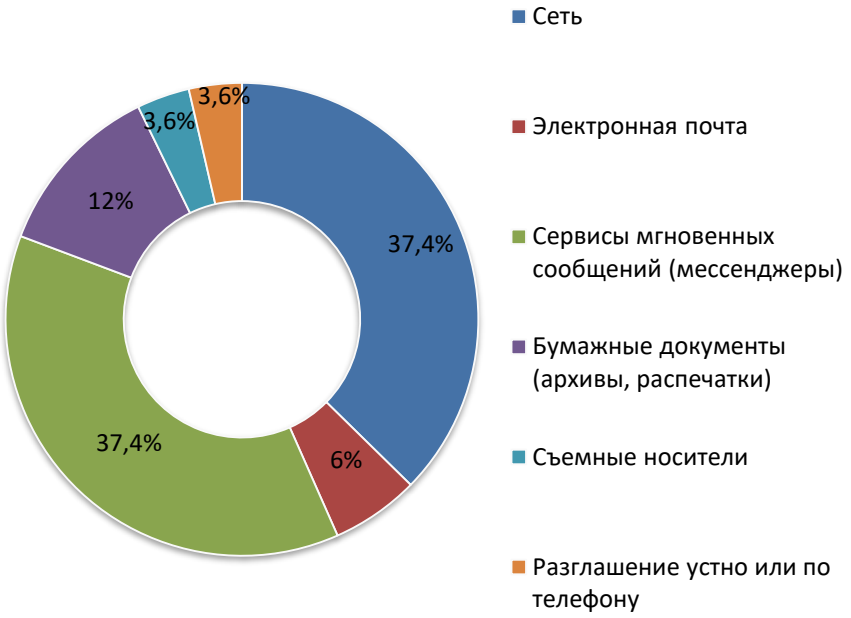

Рисунок 5. Распределение каналов передачи информации. Сведения из дел по ст. 183 УК РФ, 2019-2021 гг.

Как мы уже отмечали, исследование доступных материалов уголовных дел по статье 183 УК РФ показало, что в подавляющем большинстве случаев осужденные в момент совершения преступления занимали должности рядовых сотрудников, как правило, менеджеров в компаниях связи или в банках. (Рисунок 6).

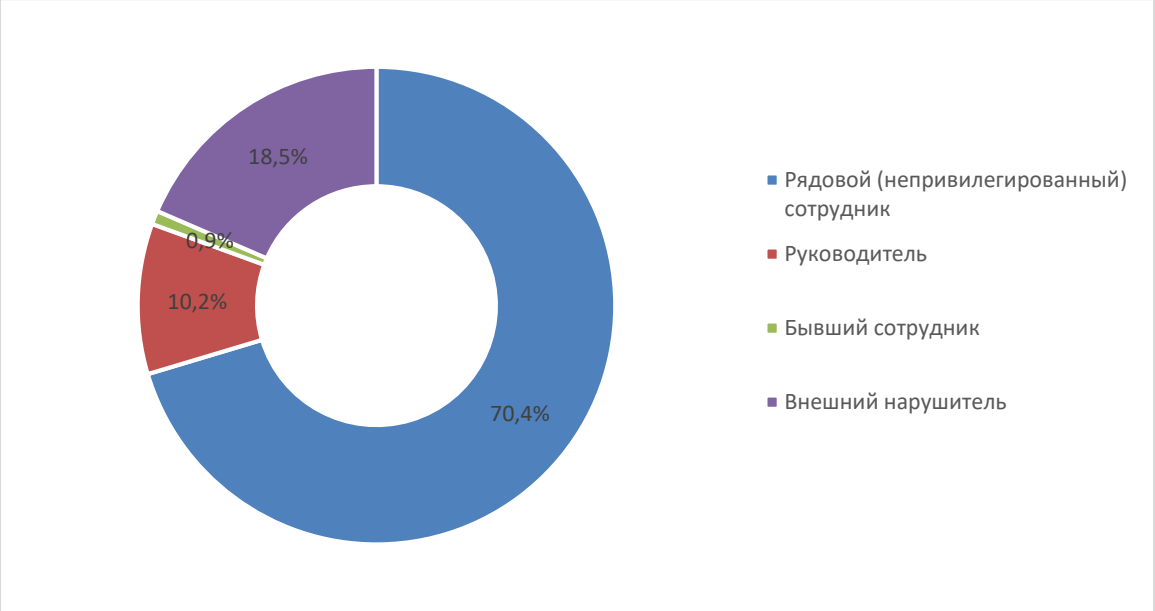

Рисунок 6. Категории подсудимых. Сведения из дел по ст. 183 УК РФ, 2019-2021 гг.

Распределение пострадавших компаний по отраслям показано на Рисунке 7.

Рисунок 7. Распределение пострадавших компаний и организаций по отраслевым группам. Сведения из дел по ст. 183 УК РФ, 2019-2021 гг.

Как писали выше, основные пострадавшие компании относятся к операторам связи и финансов, на третьем месте – промышленность.

На рисунке 8 приведено географическое распределение рассмотренных в 2019-2021 гг. дел по статье 183 УК РФ. Наибольшее количество дел рассмотрено судами Свердловской области. Далее идут Челябинская область и Республика Башкортостан. В Москве не рассмотрено ни одного дела (в Московской области три дела).

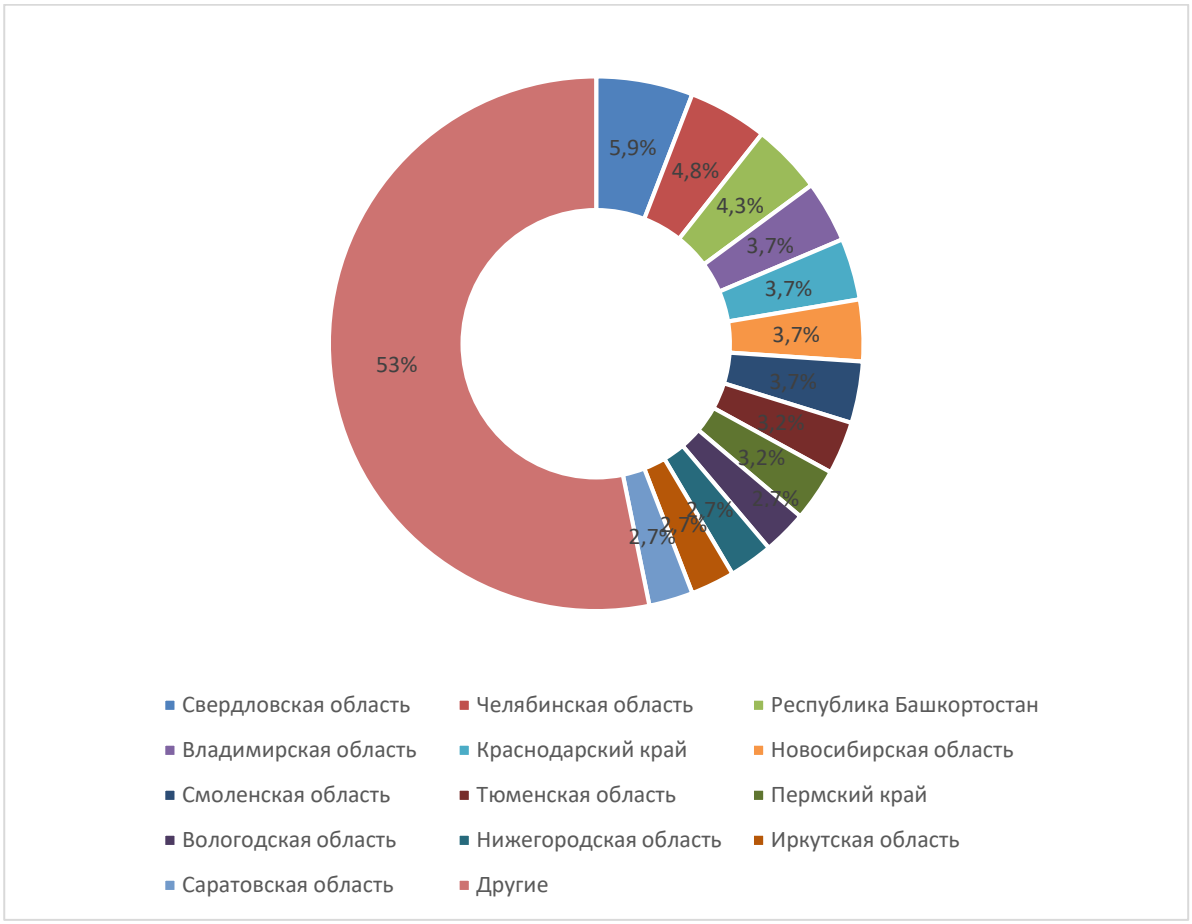

Рисунок 8. Распределение рассмотренных дел по регионам. Сведения из дел по ст. 183 УК РФ, 2019-2021 гг.

Выводы

Среди общего количества осужденных в 2019-2021 гг. за преступления в сфере экономической деятельности (глава 22 УК РФ) – более 22 тыс. человек, – количество осужденных по статье 183 УК РФ составляет примерно 0,5%. Но небольшой удельный вес нисколько не снижает значимость и общественную опасность преступлений, связанных с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайны. Особенно в эпоху, когда информация становится основным продуктом и её стоимость порой во много раз превышает стоимость материальных активов.

Исследование доступных материалов уголовных дел по статье 183 УК РФ позволило сделать вывод о том, что почти в половине случаев эти дела дополнительно классифицируются по другим статьям, особенно часто по статье 272 УК РФ «Неправомерный доступ к компьютерной информации». То есть в ходе следствия и предъявляемого обвинения статьи 183 УК РФ и 272 УК РФ часто идут «рука об руку».

Обвинительными приговорами завершились менее половины рассмотренных в последние три года дел, менее 10% приговоров были связаны с назначением реального тюремного заключения, более чем в 80% случаев судьи ограничивались назначением штрафа или условного срока.

При этом обращает на себя внимание тот факт, что прекращение уголовного дела далеко не всегда означает нулевую ответственность. Зачастую судьи назначают фигурантам дел судебные штрафы – 25 штрафов из 188 уголовных дел (13,3%).

Преступления по статье 183 УК РФ имеют ярко выраженную отраслевую направленность. В более чем 80% случаев кража коммерческой тайны, другой охраняемой законом информации совершалась из финансовых компаний и операторов связи.

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
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

Глоссарий

ГАС «Правосудие» - Государственная автоматизированная система Российской Федерации.
Запись в ГАС «Правосудие» - запись на сайте https://bsr.sudrf.ru/, включающая информацию об одном судебном решении.
Судебное дело – совокупность судебных решений всех инстанций, которые относятся к одному факту нарушения Уголовного Кодекса.

Критическая информационная инфраструктура — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;
Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;
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.

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.

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.