**Панкратьев Вячеслав Вячеславович**

# **М Е Т О Д И Ч Е С К О Е П О С О Б И Е**

# 

**Корпоративная**

**безопасность**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**Москва**

**2023**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

*Особенности современного цифрового информационного мира и конфиденциальности в нем*

* информация существует без носителя, на котором она зафиксирована;
* информация воспринимается человеком через технические средства, а не напрямую с носителя, как было раньше;
* информация не находится в конкретном месте (отсутствие локации информации, отсутствие контура информационной безопасности и т.д.). Работа с информацией происходит удаленно;
* информационные войны, информация в настоящее время является самым грозным оружием;
* информация не обладает точностью (ошибки, искажения и т.д.);
* наличие избыточного количества информации (источников информации), информационный шум. Наличие Big Data. Усложняется поиск нужной информации;
* при работе с информацией ценность представляет не сама информация, а решения, принятые на ее основе;
* в современном информационном мире проблема не найти (получить) информацию, а проблема правильно ее использовать;
* понятие конфиденциальность все чаще применяется не как защита (отсутствие) информации, а как присутствие необходимой, но не привлекающей внимание информации;
* в настоящее время самая ценная (и охраняемая) информация это планы действий и замыслы. Текущая ситуация, как правило, не относится к конфиденциальной информации;
* появление «искусственного интеллекта» позволяющего обрабатывать большие массивы информации и предлагать решения. Появление машинного обучения;
* интернет вещей, который используется для контроля за человеком;
* формирование цифрового профиля гражданина для контроля за человеком и воздействия на него;
* вся информация находится в информационных системах;
* информация не обладает объективностью (обычно присутствует субъективность);
* отсутствует однозначное понятие правда-ложь (присутствует полуправда, недосказанность, комбинация правды и лжи, фейковые новости и т.д.);
* конфиденциальная информация характеризуется следующими параметрами - ценность (стоимость) информации, время жизни информации, удобство (быстрота принятия решения) и конфиденциальность;
* подавляющее большинство информации генерируется не человеком (автоматические программы, боты и т.д.);
* неурегулированность законодательства, определяющего информационное право (например, непонятно, что такое служебная тайна) и противоречивость (коллизионность) отдельных законодательных требований (нельзя обеспечить конфиденциальность при дистанционной работе);
* значимые решения принимаются на основе той информации, доступ к которой большинство пользователей не имеют;
* импортозамещение информационных технологий и информационных систем;
* идентификация человека происходит по биометрической информации;
* информацию сложно проверить, приходится доверять или не доверять;
* на основе информации формируется мнение, осуществляется манипулирование и принимаются решения;
* деформация восприятия информации человеком в современном мире (клиповое мышление, неумение отличить правду от лжи, неумение воспринимать большое количество информации, дефицит внимания и т.д.);
* разрозненность информации (отсутствие целостности);
* увеличение мощностей технических средств обрабатывающих информацию и количества уязвимости в них;
* большая зависимость информации и принятия решений от настроек информационных систем

*Таким образом:*

* информация не может быть воспринята органами чувств, она находится неизвестно где (нигде), она нематериальна, неточна и неполна. Но она формирует мнение и на основе ее принимаются решения;
* понятие информационная безопасность включает в себя не только защиту информации и информационно-телекоммуникационных систем, но и защиту от информации;
* информация представляет собой как «оружие», так и угрозу для предприятия;
* организации, участвующие в предоставлении услуг в сфере информационной безопасности хотят заработать денег, а не защитить информацию;
* производители и разработчики ИТ программ (в том числе в сфере информационной безопасности) не несут юридической ответственности за некачественное программное обеспечение или техническое решение;
* самое слабое звено в информационной безопасности является человек и человеческий фактор;
* неверно утверждение, что цифровизация бизнес процессов позволит снизить затраты и повысить производительность труда. В итоге оцифрованный процесс становится дороже и может привести к потере управляемости в бизнес процессах;
* неверно утверждение, что при увеличении бюджета информационной безопасности растет уровень надежности и эффективности системы информационной безопасности. Прочность информационной безопасности определяется самым слабым звеном, которым, как правило, является человек;
* неверно утверждение, что своевременное обновление программного обеспечения улучшает уровень информационной безопасности. Как правило, закрывают уязвимости, которыми уже воспользовались злоумышленники. И после обновления, возможно, появились новые уязвимости;
* подавляющее количество информации в организации является информационным мусором, который нужно уничтожать, а не защищать

*Тенденции:*

* облачные хранилища и облачная обработка информации не является надежной (юрисдикция, санкции, отключения, шифрование и т.д.);
* специальные службы (и российские и других стран) имеют доступ к информации (официально или неофициально через специальные бэкдоры в программах или оборудовании);

*Искусственный интеллект* - комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру (в том числе информационные системы, информационно-телекоммуникационные сети, иные технические средства обработки информации), программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений

***Общие положения по информационной безопасности***

Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29 Конституции РФ) Исключение:

* обработка информации, доступ к которой ограничен федеральными законами
* обработка информации незаконными способами (например, с использованием специальных технических средств, предназначенных для негласного получения информации);
* обработка информации иностранными агентами

*Источниками конфиденциальной информации считаются:*

* физические лица (работники, клиенты, посетители, обслуживающий персонал);
* документы (материальные и электронные);
* технические средства носителей информации и их обработки;
* выпускаемая продукция;
* производственные и промышленные отходы

*Составляющие информационной безопасности:*

* конфиденциальность;
* доступность;
* целостность

*Каналы утечки конфиденциальной информации (через организацию деятельности)*

* взаимоотношения с физическими лицами;
* взаимоотношения с юридическими лицами;
* взаимоотношения с государственными органами;
* проведение переговоров;
* посещения территории предприятия;
* документооборот;
* реклама, выставки, публикации в печати, интервью для прессы

*Каналы утечки конфиденциальной информации (через технические средства)*

* акустический канал утечки информации;
* визуальный канал утечки информации;
* несанкционированный доступ в информационную систему;
* побочные электромагнитные излучения и наводки

*Каналы утечки конфиденциальной информации (через человеческий фактор)*

* через работников предприятия (работающих и уволенных) - умысел, неосторожность, методы социальной инженерии и т.д.;
* через физических лиц, с которыми у предприятия гражданско-правовые отношения (ИП, самозанятые и т.д.);
* через работников других организаций, с которыми у предприятия существуют (существовали) договорные отношения;
* через уволившихся работников других организаций, с которыми у предприятия существуют (существовали) договорные отношения

# *Меры по защите информации:*

* правовые меры (создание режимов, например, коммерческой тайны, патентов, авторских прав и т.д.);
* меры, связанные с кадровой работой (подбор, обучение, увольнение, контроль, действие во внештатных ситуациях, профессионализм и т.д.);
* создание конфиденциального делопроизводства (создание, хранение, уничтожение, передача документов и т.д.);
* режимные мероприятия (пропускной режим, внос-вынос документов, использование гаджетов на территории, удаленный доступ, охрана, доступ к информации и т.д.);
* организационные мероприятия (разбивание информации на части, дублирование на ключевых точках, использование облачных систем хранения, банковских ячеек, резервное копирование, аудит ИТ безопасности и т.д.);
* мероприятия по инженерно-технической защите (защита помещений, мест хранения информации, сигнализации, видеонаблюдение и т.д.);
* мероприятия по применению технических средств защиты информации (DLP – системы, шифрование, правильная настройка оборудования, защищенное программное обеспечение и т.д.).

*Подготовительные мероприятия перед защитой информации:*

* определение, какая информация подлежит или нуждается в защите;
* оптимизация защищаемых информационных потоков;
* определение формы защищаемой информации;
* определение рисков защищаемой информации и вариантов их реализации;
* определение кому может быть интересна защищаемая информация;
* определение контура информационной безопасности (как правило, он размыт);
* определение целей – реальная защита информации или формальное выполнение требований законодательства по ее защите;
* определить будем ли мы защищать информацию и информационные системы или защищать только информационные системы или только информацию;
* определить входит ли задача определения достоверности информации и защита от манипулирования в понятие информационная безопасность;
* определить время актуальности защищаемой информации.

*На что обратить внимание:*

* удаленную работу работников;
* работа с черновиками до регистрации конфиденциальных документов;
* фотографирование злоумышленниками мониторов и документов;
* мотивация персонала на неразглашение конфиденциальной информации;
* работу с информацией (носителями информации) в присутствии посторонних людей;
* природную болтливость отдельных работников;
* использование «гаджетов» на территории предприятия;
* фишинговые атаки (в основном используют чувство страха и любопытства);
* удаленный доступ к информации;
* психологические приемы для разглашения информации (социальная инженерия);
* сочетание трудовых отношений с ИТ специалистом и гражданского договора с внешней организацией;
* работа с Wi-Fi;
* настройка программного оборудования (особенно после обновления);
* импортозамещение технических решений в области информационной безопасности;
* надежность и порядочность ИТ специалиста и лиц, допущенных к конфиденциальной информации;
* разграничение доступа к информации;
* разбивание информации на части;
* включение в правовые режимы той информации, которую готовы потерять

*Принципы информационной безопасности*

* «принцип системности». К информационной безопасности надо подходить системно, комплексно. Это отбор персонала и его обучение, создание регламентов работы на предприятии, защита информационной системы и т.д.;
* «принцип информационного шума». Ценная информация должна сопровождаться большим количеством информационного шума, чтобы было сложно ее выделить из общей информационной массы;
* «принцип разделяй и властвуй». Информация разделяется на части и распределяется между разными работниками, желательно территориальное разделение.

### *Правовые основы информационной безопасности на предприятии*

*Информационные ресурсы делятся:*

* общедоступная информация
* общедоступная по закону;
* общедоступная по инициативе обладателя информации
* информация с ограниченным доступом (доступ ограничивается федеральным законом)
* государственная тайна;
* конфиденциальная информация;
* информация, не имеющая классификации, но распространение которой ограничивается законом (например, обмен информацией при торгах и т.д.)

*Информация в зависимости от порядка ее предоставления подразделяется на:*

* информацию, свободно распространяемую;
* информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
* информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
* информацию, распространение которой в РФ ограничивается или запрещается.

*Не может быть ограничен доступ к:*

* нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
* информации о состоянии окружающей среды;
* информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную [тайну](https://login.consultant.ru/link/?req=doc&base=LAW&n=93980&date=25.04.2020&dst=100003&fld=134));
* информации, накапливаемой в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
* информации, содержащейся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством РФ);
* иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

*К конфиденциальной информации относится (по Указу Президента РФ от 06.03.1997 г. № 188):*

* сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);
* сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, попадающих под действие законов о защите судей, должностных лиц правоохранительных и контролирующих органов, потерпевших, свидетелей и иных участников уголовного судопроизводства;
* служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
* сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
* сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);
* сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;
* сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц

*ФЗ "Об информации, информационных технологиях и защите информации"* установил:

* информация – это сведения (сообщения, данные) независимо от формы их представления (нет привязки к материальным носителям);
* свободу поиска, получения, передачи, производства и распространения информации любым законным способом т.е. граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований федеральных законов;
* ограничения доступа к информации только федеральными законами, а так же обязательность соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами;
* какая информация предоставляется бесплатно (о деятельности госорганов, затрагивающая права и обязанности заинтересованного лица и т.д.);
* неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица);
* информация может являться объектом публичных, гражданских и иных правовых отношений;
* обладателем информации (лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации) может быть физическое лицо, юридическое лицо, государственный орган и т.д.;
* обладатель информации вправе:
* разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
* использовать информацию, в том числе распространять ее, по своему усмотрению;
* передавать информацию другим лицам по договору или на ином установленном законом основании;
* защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
* осуществлять иные действия с информацией или разрешать осуществление таких действий.
* обладатель информации при осуществлении своих прав обязан:
* соблюдать права и законные интересы иных лиц;
* принимать меры по защите информации;
* ограничивать доступ к информации, если такая обязанность установлена федеральными законами.
* в случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством;
* электронное сообщение, подписанное цифровой подписью, признается электронным документом, равнозначным документу, подписанному собственноручной подписью;
* в целях заключения гражданско-правовых договоров обмен электронными сообщениями, каждое из которых подписано цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, рассматривается как обмен документами;
* возможность формировать информационные системы, при этом оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных;
* защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа,
* реализацию права на доступ к информации.
* обладатель информации, оператор информационной системы в случаях, установленных законодательством РФ, обязаны обеспечить:
* предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
* своевременное обнаружение фактов несанкционированного доступа к информации;
* предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
* недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
* возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

### постоянный контроль за обеспечением уровня защищенности информации.

### лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством РФ требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

***Защита персональных данных***

*Общее понимание терминов и ситуации*

* ФЗ «О персональных данных» регулируются отношения, связанные с обработкой ПД, осуществляемой органами государственной власти, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами. Законом не регулируются отношения, связанные с обработкой ПД физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права других субъектов ПД;
* ПД могут быть:
* *предоставленные ПД* – полученные от субъектов ПД или их представителей, например, заполнение вебформы на сайте, предоставление резюме и т.д.;
* *распространенные ПД* – взятые из общедоступных или открытых источников, например, исследование учетных записей в социальных сетях;
* *наблюдаемые ПД* – зафиксированы путем отслеживания поведения субъектов ПД, например, онлайн трекинг, отслеживание посещаемости занятий, геолокация, видеонаблюдение и т.д.;
* *принятые ПД* – полученные не от субъектов ПД или их представителей, а от других лиц, например, рекомендация от бывшего работодателя соискателя;
* *инициированные ПД* – образованы в отношении действий субъектов ПД, например выплата зарплаты, угон личного автомобиля и т.д.;
* *назначенные ПД* – временно или постоянно присвоены субъектам ПД, например номер социального страхования, наименование должности, сертификат об обучении и т.д.;
* *производные ПД* – синтезированы в результате простого анализа других данных, например, расчет прибыльности клиента путем по количеству посещений и купленных товаров;
* *предполагаемые ПД* – спрогнозированы после продвинутого анализа набора данных, например, расчет кредитного рейтинга или прогнозирование состояния здоровья
* нет единого закона, который бы охватил весь спектр юридических вопросов по защите ПД;
* не проработан вопрос о том, как обрабатывать ПД при удаленной работе;
* ФЗ «О персональных данных» необходимо рассматривать во взаимоотношениях с другими федеральными законами;
* нет единого перечня сведений, составляющих ПД человека;
* существуют противоречия (неурегулированность) в самом законе о ПД. Все ПД относятся к конфиденциальным, но есть понятие общедоступные ПД. Не урегулирован вопрос снятия режима конфиденциальности с ПД;
* ПД могут быть в любой форме – текстовой, цифровой, графической, видео или акустической. Сюда входит все: и информация, зафиксированная на бумаге, и информация, хранимая в памяти компьютера в двоичной виде, в виде звука или изображения;
* важную смысловую нагрузку в определении ФЗ «О персональных данных» несет слово «относящаяся». Это информация, относятся не только «к лицу», но и информация «о лице». К примеру, при приеме на работу HR-менеджер заполняет кадровую форму Т-2, в которой указываются сведения о родственниках. И эти ПД уже будут «относиться» не только к родственникам работника, но также и к самому работнику;
* статус «персональные данные» постоянный, в отличие от статуса «коммерческая тайна» или «государственная тайна», которые могут быть сняты;
* на документах, в которых есть персональные данные нет ограничительной пометки, в отличие от документов с государственной, коммерческой или служебной тайной;
* персональные данные могут быть общедоступные, в отличие от государственной или коммерческой тайны;
* персональные данные могут относиться к иным видам тайн (государственной, коммерческой, банковской, адвокатской и т.д.);
* отличие понятия «*распространения ПД*» и «*предоставление ПД*». В определении «распространение» ключевым словом является «неопределенному» кругу лиц. То есть это действие, когда ПД передаются всем. Ключевым словом в определении «предоставление» является «определенному». То есть, пусть и широкому, но вполне конкретному составу лиц. При распространении ПД закон требует получения согласия субъекта и это основное требование соблюдения конфиденциальности ПД. А для предоставления ПД такого такое согласие закон требует не всегда;
* предоставление ПД может быть обязательным (по закону) и добровольным. При обязательном предоставлении ПД согласие субъекта не требуется;
* есть понятие «обезличивание ПД», но нет понятия обезличенные ПД. Обезличивание ПД – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному человеку. ПД после процедуры обезличивания перестают быть персональными и к ним не предъявляются требования ФЗ-152;
* *«биометрические ПД»*– сведения, которые *характеризуют* физиологические и биологические особенности человека, на основании которых *можно установить* его личность и которые используются оператором для установления личности субъекта.

Термин *«характеризует*» говорит о том, что все сведения, которые так или иначе отражают физиологию или биологические особенности - это биометрические ПД.

Термин «*на основании которых можно установить*» оговаривает возможность, а не факт установления личности субъекта, то есть это не одно и то же, что «позволяют установить личность». По отпечатку пальца (как и по фото) можно установить личность только в том случае, если где-то существует база данных, в которой этот отпечаток сопоставляется с идентификационными данными субъекта. То есть биометрические данные служат идентификатором субъекта, но не идентифицируют его.

* фото и видео изображение попадает под действие ФЗ «О персональных данных»:

Статья 1521 ГК РФ «Охрана изображения гражданина» устанавливает, что обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. Такое согласие не требуется в случаях, когда использование изображения осуществляется в государственных, общественных или иных публичных интересах, изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях, а так же если гражданин позировал за плату.

* понятие «*согласие*» в ФЗ «О персональных данных». Согласие на обработку ПД должно быть конкретным, информированным и сознательным. Согласие на обработку ПД может быть дано субъектом ПД или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законом;

Обязанность предоставить доказательство получения согласия субъекта на обработку его ПД или доказательство того, что имеется случай, когда согласия субъекта не требуется, возлагается на оператора.

Есть юридическое понятие «*конклюдентные действия*», то есть выражение своей воли и согласия, совершая какое-то определенное, заранее оговоренное действие (например, бросаем деньги в автомат для покупки кофе, прикладываем банковскую карточку к терминалу и т.д.). Или прочитывая информацию на экране компьютера и ставя галочку, что согласны с текстом;

Конклюдентные действия при получении согласия текст - «Уважаемые посетители! Передавая оператору бюро пропусков документ, удостоверяющий личность, Вы совершаете конклюдентное действие, свидетельствующее о Вашем согласии на обработку персональных данных»;

Также есть понятие электронный документ и информация в электронной форме. Информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью;

* термин *«оператор ПД»*– государственный орган, муниципальный орган, юридическое или физическое лицо, которое самостоятельно или совместно с другими лицами организует и (или) осуществляет обработку данных и определяет цели обработки ПД, состав ПД, подлежащих обработке, действия, совершаемые с персональными данными;

Из смысла понятия «оператор» следует, что порядок обработки и защиты ПД, установленный законом, не распространяется на тех, кто не является юридическим лицом. Если ПД обрабатываются самим субъектом исключительно для личных и семейных нужд и если при этом не нарушаются права других субъектов, то каждый имеет право поступать так, как хочет.

* *аутсорсинг обработки ПД.* Оператор вправе поручить обработку ПД другому лицу с согласия субъекта, на основании заключаемого с этим лицом договора (поручения).

Разделена ответственность между оператором и третьим лицом. Оператор отвечает перед субъектом, третье лицо по регрессу отвечает перед оператором. В случае, если оператор поручает обработку ПД другому лицу, ответственность перед субъектом ПД за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

В договоре на аутсорсинг обработки ПД необходимо включить:

* перечень действий (операций) с ПД;
* цель обработки и состав данных, подлежащих обработке;
* обязанность соблюдать конфиденциальность в работе с ПД;
* обязанность обеспечивать безопасность ПД и требования к защите обрабатываемых ПД;
* регламентация процедур контроля со стороны оператора за обработкой ПД;
* обязанность соблюдения законных принципов обработки ПД;
* обязанность обеспечения безопасности ПД;
* обязанность не раскрывать / не распространять ПД;
* обязанность принять технические и организационные меры защиты ПД;
* обязанность установить правила доступа к ПД;
* обязанность провести оценку эффективности мер защиты ПД;
* право оператора осуществлять проверку порядка обработки ПД;
* санкции за нарушение порядка обработки ПД;
* уровень защищенности ПД, подлежащий обеспечению;
* порядок уничтожения ПД по завершении их обработки;
* порядок оценки эффективности принятых мер защиты

*ФЗ «О персональных данных»* установил, что:

* персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
* персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
* в ФЗ «О персональных данных» есть отдельная глава, регламентирующая работу с ПД, разрешенными субъектом ПД для распространения;
* субъект ПД принимает решение о предоставлении его ПД и дает согласие на их обработку свободно, своей волей и в своем интересе и это согласие может быть отозвано субъектом ПД;
* оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законом и принятыми в соответствии с ним нормативными правовыми актами;
* к мерам по защите ПД могут относиться:
* назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки ПД;
* издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки ПД;
* применение правовых, организационных и технических мер по обеспечению безопасности ПД в соответствии c законом;
* осуществление внутреннего контроля и (или) аудита соответствия обработки ПД закону и принятым в соответствии с ним нормативным правовым актам;
* оценка вреда, который может быть причинен субъектам ПД в случае нарушения закона, соотношение указанного вреда и принимаемых оператором мер;
* ознакомление работников оператора, осуществляющих обработку ПД, с положениями закона и локальными актами по вопросам обработки ПД, и (или) обучение указанных работников
* оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
* при сборе ПД, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПД граждан РФ с использованием баз данных, находящихся на территории РФ (есть исключение);
* оператор при обработке ПД обязан принимать необходимые правовые, организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД;
* безопасность ПД достигается:
* определением угроз безопасности ПД при их обработке в информационных системах ПД;
* применением организационных и технических мер по обеспечению безопасности ПД при их обработке в информационных системах ПД;
* применением прошедших процедуру оценки соответствия средств защиты информации;
* оценкой эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию информационной системы ПД;
* учетом машинных носителей ПД;
* обнаружением фактов несанкционированного доступа к ПД и принятием мер;
* восстановлением ПД, модифицированных или уничтоженных вследствии несанкционированного доступа к ним;
* установлением правил доступа к ПД, обрабатываемым в информационной системе ПД, а также обеспечением регистрации и учета всех действий, совершаемых с ПД в информационной системе ПД;
* контролем за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности информационных систем ПД.
* контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПД, при обработке ПД в государственных информационных системах персональных данных осуществляются Роскомнадзором и ФСТЭК без права ознакомления с ПД, обрабатываемыми в информационных системах ПД;
* в случае достижения цели обработки ПД оператор обязан прекратить обработку ПД и уничтожить ПД в срок, не превышающий тридцати дней с даты достижения цели обработки ПД, если иное не предусмотрено договором;
* оператор до начала обработки ПД обязан уведомить уполномоченный орган по защите прав субъектов ПД о своем намерении осуществлять обработку ПД, за исключением случаев, предусмотренных законом;
* оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки ПД;
* лицо, ответственное за организацию обработки ПД, в частности, обязано:
* осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства о ПД;
* доводить до сведения работников оператора положения законодательства о ПД, локальных актов по вопросам обработки ПД, требований к защите ПД;
* организовывать прием и обработку обращений и запросов субъектов ПД или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

*Изменения в законодательстве о ПД с 01.09.2022*

* срок ответа Роскомнадзору сократили с 30 календарных [до 10 рабочих дней](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100079&field=134). Он может быть увеличен в пределах 5 рабочих дней на основании мотивированного уведомления;
* из закона о ПД [исключили](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100092&field=134) большинство случаев, когда организациям не нужно было уведомлять Роскомнадзор о намерении начать обрабатывать ПД;
* с 1 марта 2023 года изменяется порядок трансграничной передачи ПД. Требуется уведомить Роскомнадзор о трансграничной передаче ПД;
* если для обработки ПД не используют средства автоматизации, уведомлять ведомство [не нужно](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=12.10.2022&dst=90&field=134). Например, данные о посетителях организации записывают в бумажный журнал при выдаче им разовых пропусков;
* Роскомнадзор [указал](https://login.consultant.ru/link/?req=doc&base=LAW&n=425663&date=12.10.2022&dst=100004&field=134): уведомление нужно подать также и тем, кто уже обрабатывал ПД в ситуациях, которые ранее считались исключением. Крайний срок подачи уведомления [не определен](https://login.consultant.ru/link/?req=doc&base=LAW&n=425663&date=12.10.2022&dst=100011&field=134);
* скорректировали требования к содержанию уведомления. Если ПД будут обрабатывать в разных целях, то для каждой из них [понадобится указать](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100100&field=134):
* категорию ПД и их субъектов;
* правовое основание обработки ПД;
* перечень действий с ПД и способы их обработки.
* в законе о ПД [закрепили](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100106&field=134) положение о том, что формы уведомлений должен установить Роскомнадзор;
* в законе о ПД [конкретизировали](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100068&field=134) требование о том, что локальные акты оператора должны содержать:
* категории и перечни обрабатываемых данных;
* категории субъектов данных;
* способы и сроки обработки, хранения данных;
* порядок их уничтожения.
* в законе о ПД определили обязанности оператора в случае компрометации персональных данных. У оператора есть [24 часа](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100082&field=134) с момента происшествия, чтобы сообщить в Роскомнадзор:
* об инциденте;
* о предполагаемой причине и вреде, причиненном субъектам ПД;
* о мерах по устранению последствий инцидента;
* о представителе организации, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с происшествием.
* в законе о ПД определили обязанности оператора в случае компрометации персональных данных. У оператора есть [72 часа](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100084&field=134) с момента инцидента, чтобы провести внутреннее расследование и сообщить в Роскомнадзор о его результатах, а также о виновниках (при наличии). На сайте Роскомнадзора доступны специальные электронные формы подачи уведомлений;
* оператор ПД [обязан](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100073&field=134) взаимодействовать с госсистемой обнаружения компьютерных атак ([ГосСОПКА](https://login.consultant.ru/link/?req=doc&base=LAW&n=220885&date=12.10.2022&dst=100028&field=134)), в том числе направлять сообщения об утечке данных;
* закон о ПД уточнил содержание поручения обработки ПД другому лицу.В поручении [нужно дополнительно отразить](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100016&field=134):
* перечень ПД;
* [обязанность](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=12.10.2022&dst=14&field=134) использовать для записи и хранения ПД базы данных на территории РФ;
* [меры](https://login.consultant.ru/link/?req=doc&base=LAW&n=422241&date=12.10.2022&dst=100357&field=134), которые должен предпринять исполнитель для выполнения требований закона о ПД;
* обязанность по запросу предоставлять в течение срока действия поручения информацию о соблюдении условий обработки ПД;
* обязанность уведомить о случаях компрометации обрабатываемых данных.
* закон о ПД уточнил содержание согласия на обработку ПД. В число требований к согласию [включили](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100020&field=134) то, что оно должно быть предметным и однозначным. Если получение согласия обязательно, [компания должна разъяснить](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100061&field=134) физлицу последствия не только отказа в предоставлении ПД, но и отказа дать согласие на их обработку;
* закон о ПД уточнил предоставление информации физлицам об обработке их ПД. Перечень сведений [дополнили](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100058&field=134) информацией о том, какими способами оператор выполняет обязанности, предусмотренные законом о ПД;
* по запросу гражданина или его представителя сведения об обработке его ПД нужно предоставить в течение [10 рабочих дней](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100057&field=134). Срок может быть увеличен в пределах 5 рабочих дней на основании мотивированного уведомления. Ответ дается в той же форме, в какой поступил запрос, если в запросе не указано иное;
* закон о ПД уточнил процедуры прекращения обработки ПД по требованию физлица. У оператора есть 10 рабочих дней с момента получения требования физлица, чтобы [прекратить обработку](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100085&field=134) ПД о нем или обеспечить прекращение обработки (если ее ведет другое лицо). Срок можно продлить в пределах 5 рабочих дней на основании мотивированного уведомления;
* закон о ПД уточнил особенности обработки ПД потребителей. По общему правилу продавец [не может отказать](https://login.consultant.ru/link/?req=doc&base=LAW&n=416194&date=12.10.2022&dst=100035&field=134) потребителю в заключении, исполнении, изменении или расторжении договора из-за отказа потребителя предоставить персональные данные. Есть два исключения:
* данные нужны для исполнения договора;
* предоставить данные требует закон.
* за нарушение данного требования продавца [могут оштрафовать](https://login.consultant.ru/link/?req=doc&base=LAW&n=417857&date=12.10.2022&dst=100009&field=134): должностных лиц на сумму от 5 000 до 10 000, юридических лиц - от 30 000 до 50 000;
* если потребитель потребует объяснить, почему из-за непредставления ПД ему отказали в заключении, исполнении, изменении или расторжении договора, ответить нужно в течение [7 дней](https://login.consultant.ru/link/?req=doc&base=LAW&n=416194&date=12.10.2022&dst=100036&field=134), при устном запросе - [незамедлительно](https://login.consultant.ru/link/?req=doc&base=LAW&n=416194&date=12.10.2022&dst=100038&field=134);
* нельзя отказывать в обслуживании физическому лицу, если оно не хочет предоставлять биометрические ПД или соглашаться на обработку ПД, а закон не требует от организации получать такое согласие;
* закон о ПД регламентировал использование ПД иностранными лицами. Положения закона о ПД [распространили](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100010&field=134) на иностранные компании и физических лиц, которые используют данные российских физических лиц (например, по договору). Если компания [передала данные](https://login.consultant.ru/link/?req=doc&base=LAW&n=421898&date=12.10.2022&dst=100019&field=134) иностранной организации для обработки, ответственность перед физлицом несут обе организации.

*Биометрические ПД*

* сведения о физиологических и биологических особенностях человека
* статические сведения - физиологическая характеристика человека, т.е. уникальное свойство, данное человеку от рождения, например: рисунок вен; папиллярные узоры пальцев; радужная оболочка и сетчатка глаза; геномная информация; фотография или видеоизображение лица.
* динамические сведения - поведенческая характеристика человека, например: голос; подпись, показывающая физиологическо-поведенческие характеристики (степень нажатия, направление движений, штрих и прочие аспекты); поведенческие паттерны (например, нажатие клавиш).
* позволяют установить личность человека
* оператор должен организовывать и, возможно, осуществлять обработку биометрических данных, т.е. если такие данные обрабатываются исключительно на устройстве пользователя, а оператору сообщаются лишь сведения о результатах идентификации, то нельзя говорить об обработке оператором биометрических данных. В законодательстве РФ не указывается на достоверную идентификацию субъекта как на необходимый признак биометрических данных, хотя наличие ошибок идентификации неизбежно. Все биометрические технологии характеризуются таким параметрами, как False Accept Rate (процент ошибочного разрешения доступа) и False Reject Rate (процент ошибочного отказа в доступе). Следует применять специальные технические средства для анализа биометрических данных и их сопоставления с эталонными образцами.
* используются оператором для установления личности субъекта ПД
* биометрическая аутентификация — процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путём преобразования этого образа в соответствии с заранее определённым протоколом аутентификации. Не следует путать данные системы с системами биометрической идентификации, каковыми являются, к примеру системы распознавания лиц водителей и биометрические средства учёта рабочего времени. Биометрические системы аутентификации работают в активном, а не пассивном режиме и почти всегда подразумевают авторизацию. Хотя данные системы не идентичны системам авторизации, они часто используются совместно (например, в дверных замках с проверкой отпечатка пальца).

*Подготовительные мероприятия по защите ПД на предприятии*

* анализ ситуации по обработке ПД;
* определение - кто будет заниматься защитой ПД (своими силами или силами внешних компаний);
* инвентаризация всех информационных ресурсов;
* определение - какие ПД обрабатываются (в рамках трудовых или гражданско-правовых отношений);
* определение категорий обрабатываемых ПД;
* изучение законодательства РФ и ведомственных нормативных правовых актов в области обработки ПД;
* изучение формы обработки ПД (без использования или с использованием автоматизированных систем);
* определение необходимости обработки биометрических ПД;
* определение необходимости использования средств криптографической защиты информации для защиты ПД;
* определение цели защиты ПД (реальная защита или выполнение требований регуляторов).

*Организационно-правовые мероприятия по защите ПД на предприятии*

* составление плана работы по выполнению требований законодательства РФ в сфере обработки ПД;
* утверждение организационно-распорядительных документов по обработке ПД;
* назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки ПД;
* составление перечня обрабатываемых ПД;
* получение согласия субъектов на обработку ПД;
* направление уведомления в Роскомнадзор о своем намерении осуществлять обработку ПД;
* определение сроков обработки ПД;
* определение целей обработки ПД;
* определение порядка обработки ПД (получение, учет, хранение, защита, обезличивание, уничтожение и т.д.);
* определение должностных лиц, допущенных к работе с ПД и их полномочий по работе с ними;
* определение помещений, в которых будут обрабатываться ПД;
* доведение до персонала требований безопасности при обработке ПД;
* обучение персонала правилам работы с ПД;
* создание системы внутреннего контроля за обработкой ПД.

*Технические мероприятия по защите ПД*

* обследование существующей информационной системы на предмет возможности использовать ее для обработки ПД;
* разработка технического задания на создание (модернизацию) ИСПД;
* проектирование и создание ИСПД;
* введение в эксплуатацию ИСПД;
* формирование модели угроз безопасности ПД при их обработке в ИСПД;
* классификация ИСПД;
* создание системы учета ИСПД и машинных носителей ПД;
* выполнение требований положения о методах и способах защиты информации в ИСПД в зависимости от класса системы и модели угроз безопасности;
* выполнение требований безопасности ПД при применении средств криптографической защиты информации;
* выполнение требований по инженерной защите помещений, в которых обрабатываются ПД.

*Организационно-распорядительная документация по обработке ПД включает в себя:*

* перечень ПД, подлежащих защите;
* перечень помещений (мест хранения) ПД;
* уведомление Роскомнадзора о начале обработке ПД;
* назначение должностного лица (подразделения), ответственного за обработку ПД в организации;
* политика обработки ПД;
* модель угроз безопасности ПД в ИСПД;
* перечень ИСПД с назначением ответственных за безопасность информации в них и установление уровней защищенности ПД;
* перечень должностей, допущенных к обработке ПД;
* регламент взаимодействия с субъектами ПД (включая раздел по взаимодействию с субъектами при передаче их ПД третьей стороне);
* регламент взаимодействия с уполномоченными органами;
* инструкции администраторов безопасности ПД;
* инструкции пользователей при работе с ПД;
* обязательства о соблюдении режима конфиденциальности ПД работников;
* типовая форма согласия субъекта на обработку ПД;
* типовая форма согласия субъекта на передачу его ПД третьей стороне;
* типовая форма согласия субъекта ПД для распространения;
* типовая форма акта на уничтожение ПД;
* порядок уничтожения (обезличивания) ПД;
* документы, регламентирующие видеонаблюдение в организации;
* журнал учета машинных носителей ПД, средств защиты информации и т.д.;
* журнал учета обращений субъектов ПД о выполнении требований по обработке их ПД;
* журнал учета ПД, необходимых для однократного пропуска субъекта ПД на территорию, на которой находится оператор, или в иных аналогичных целях;
* журнал учета передачи ПД третьей стороне;
* акты приема-передачи документов (материальных носителей), содержащих ПД;
* план внутренних проверок по обработке ПД;
* документы, подтверждающие прохождение обучения работников требованиям по обработке ПД;
* договора (соглашения) с аутсорсинговыми организациями, обрабатывающими ПД работников

*При использовании средств криптографической защиты информации (СКЗИ) дополнительно создаются:*

* акты ввода СКЗИ в эксплуатацию;
* журнал поэкземплярного учета СКЗИ;
* приказ о порядке организации контроля за соблюдением условий использования СКЗИ;
* договоры на приобретение СКЗИ;
* сертификат на используемые СКЗИ;
* эксплуатационная документация на СКЗИ;
* приказ о назначении лиц (пользователей СКЗИ), допущенных к работе с ключами СКЗИ;
* журнал учета криптографических ключей СКЗИ;
* акты о комиссионном уничтожении криптографических ключей СКЗИ

*Государственный контроль за обработкой ПД*

*Роскомнадзор* – регулятор в области соблюдения законодательства по обработке ПД. Его основные полномочия:

* вести Реестр операторов ПД;
* требовать блокирования и уничтожения ПД, полученных незаконно или обрабатывающих с нарушением требований законодательства;
* определять перечень государств, в которых обеспечивается адекватная защита ПД;
* осуществлять государственный контроль и надзор порядка обработки ПД в организациях;
* составлять протоколы об административном правонарушении

В рамках исполнения своих функций, должностные лица Роскомнадзора имеют право:

* выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области обработки ПД;
* составлять протоколы об административном правонарушении или направлять в органы прокуратуры материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПД;
* направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии;
* принимать меры по приостановлению или прекращению обработки ПД, осуществляемой с нарушениями требований законодательства.

*ФСТЭК России* **–** регулятор в области обеспечения технической защиты ПД не криптографическими методами. Она наделена полномочиями:

* устанавливать требования по технической защите ПД;
* поводить лицензирование видов деятельности по технической защите ПД;
* организовывать и проводить сертификацию средств защиты информации;
* осуществлять контроль и надзор выполнения требований обеспечения безопасности в государственных информационных системах, обрабатывающих ПД

*ФСБ России* **–** регулятор в области использования средств криптографической защиты информации, в том числе для защиты ПД. Она наделена полномочиями:

* устанавливать требования по защите ПД криптографическими методами;
* лицензировать деятельность по использованию СКЗИ;
* организовывать и проводить сертификацию СКЗИ;
* осуществлять контроль и надзор выполнения требований обеспечения безопасности при использования СКЗИ в государственных информационных системах;

*Банк России* **–** специфический регулятор отношений в кредитно-финансовой области. Он обладает полномочиями по установлению актуальных угроз безопасности, при обработке ПД в информационных системах, эксплуатируемых кредитными организациями, а также устанавливает требования по их защите

*Ответственность за нарушение режима (разглашение) ПД, применяемая к работнику:*

* за нарушение требований к обработке ПД на работника можно наложить дисциплинарное взыскание (замечание, выговор);
* за разглашение ПД предусмотрено право работодателя уволить работника;
* если нужно привлечь за разглашение ПД к уголовной ответственности, то ПД нужно включить в коммерческую тайну предприятия

*Типичные нарушения операторами законодательства о ПД (по результатам проверок Роскомнадзора)*

* отсутствует политика оператора по обработке ПД;
* отсутствуют согласия на обработку ПД (работников, кандидатов на работу, родственников, посетителей и т.д.) или согласие составлено неправильно или неполно;
* отсутствуют согласия работников на передачу их ПД в другие организации;
* отсутствует перечень ПД оператора;
* отсутствует перечень помещений (мест хранения), в которых обрабатываются ПД;
* отсутствует перечень лиц, осуществляющих обработку ПД и имеющих доступ к ПД;
* отсутствует уведомление Роскомнадзора об обработке ПД или оно составлено неполно (неправильно);
* отсутствует должностное лицо (подразделение), ответственное за обработку ПД;
* отсутствует перечень информационных систем, в которых обрабатываются ПД;
* не определены (неправильно определены) цели обработки ПД;
* отсутствуют модели угроз ПД в автоматизированных системах обработки ПД;
* отсутствует внутренний контроль (аудит) соответствия обработки ПД требованиям законодательства;
* отсутствует ознакомление работников оператора с положениями законодательства и документами, определяющими политику оператора в отношении обработки ПД;
* отсутствует обучение работников требованиям законодательства и документов, определяющих политику оператора в отношении обработки ПД;
* лица, осуществляющие обработку ПД без использования средств автоматизации не проинформированы об этом (факт обработки ими ПД, категории обрабатываемых ПД, особенности и правила осуществления такой обработки и т.д.)

*Административная ответственность работодателя за нарушение законодательства о ПД (статья 13.11):*

* обработка ПД в случаях, не предусмотренных законодательством РФ в области ПД, либо обработка ПД, несовместимая с целями сбора ПД, за исключением случаев, предусмотренных [частью 2](#Par5) настоящей статьи, если эти действия не содержат уголовно наказуемого деяния, - влечет предупреждение или наложение административного штрафа на граждан в размере 1 000 - 3 000 рублей; на должностных лиц - 5 000 - 10 000 рублей; на ЮЛ - 30 000 - 50 000 рублей;
* обработка ПД без согласия в письменной форме субъекта ПД на обработку его ПД в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области ПД, если эти действия не содержат уголовно наказуемого деяния, либо обработка ПД с нарушением установленных законодательством РФ в области ПД требований к составу сведений, включаемых в согласие в письменной форме субъекта ПД на обработку его ПД, - влечет наложение административного штрафа на граждан в размере 3 000 - 5 000 рублей; на должностных лиц - 10 000 - 20 000 рублей; на ЮЛ - 15 000 - 75 000 рублей;
* невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки ПД, или сведениям о реализуемых требованиях к защите ПД - влечет предупреждение или наложение административного штрафа на граждан в размере 700 - 1 500 рублей; на должностных лиц - 3 000 - 6 000 рублей; на ИП - 5 000 – 10 000 рублей; на ЮЛ - 15 000 – 30 000 рублей;
* невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по предоставлению субъекту ПД информации, касающейся обработки его ПД, - влечет предупреждение или наложение административного штрафа на граждан в размере 1 000 – 2 000; на должностных лиц – 4 000 – 6 000 рублей; на ИП – 10 000 - 15 000 рублей; на ЮЛ – 20 000 – 40 000 рублей;
* невыполнение оператором в сроки, установленные законодательством РФ в области ПД, требования субъекта ПД данных об уточнении ПД, их блокировании или уничтожении в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, - влечет предупреждение или наложение административного штрафа на граждан в размере 1 000 - 2 000 рублей; на должностных лиц – 4 000 - 10 000 рублей; на ИП – 10 000 - 20 000 рублей; на ЮЛ – 25 000 – 45 000 рублей;
* невыполнение оператором при обработке ПД без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ в области ПД сохранность ПД при хранении материальных носителей ПД и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к ПД, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении ПД, при отсутствии признаков уголовно наказуемого деяния - влечет наложение административного штрафа на граждан в размере 700 – 2 000 рублей; на должностных лиц - 4 000 – 10 000 рублей; на ИП – 10 000 – 20 000 рублей; на ЮЛ – 25 000 – 50 000 рублей;
* невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ в области ПД обязанности по обезличиванию ПД либо несоблюдение установленных требований или методов по обезличиванию ПД - влечет предупреждение или наложение административного штрафа на должностных лиц в размере 3 000 – 6 000 рублей;
* невыполнение оператором при сборе ПД, в том числе посредством сети "Интернет", предусмотренной законодательством РФ в области ПД обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения ПД граждан РФ с использованием баз данных, находящихся на территории РФ, - влечет наложение административного штрафа на граждан в размере 30 000 – 50 000 рублей; на должностных лиц – 100 000 – 200 000 рублей; на ЮЛ - 1 000 000 – 6 000 000 рублей (часть 8);
* повторное совершение административного правонарушения, предусмотренного частью 8 настоящей статьи, - влечет наложение административного штрафа на граждан в размере 50 000 – 100 000 рублей; на должностных лиц – 500 000 - 800 000 рублей; на ЮЛ – 6 000 000 – 18 000 000 рублей

*Административная ответственность за  разглашение информации с ограниченным доступом (Статья 13.14 КОАП)*

* разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей - влечет наложение административного штрафа на граждан в размере 500 – 1000 рублей; на должностных лиц – 4 000 – 5 000 рублей.

*Уголовная ответственность за правонарушения в области персональных данных*

* Ст. 137 УК РФ – нарушение неприкосновенности частной жизни;
* Ст. 140 УК РФ – отказ в предоставлении гражданину информации

*Международное законодательство в области защиты ПД*

*General Data Protection Regulation (GDPR)*–это регламент ЕС о защите ПД, формирующий обязательные к соблюдению единые принципы и подходы как для государств - членов ЕС, так и для некоторых иных государств (Исландия, Лихтенштейн, Норвегия).

* GDPR имеет экстерриториальное действие и применяется ко всем компаниям, обрабатывающим ПД резидентов и граждан ЕС, независимо от местонахождения такой компании;
* разделяется понятия контроллер данных (data controller) и процессор данных (data processor). Контроллеры решают, что происходит с персональными данными и несут ответственность за обработку, а процессоры являются некими “исполнителями”. Например, облачная система, которой пользуются сотрудники для целей выполнения задач и проектов, где также хранятся персональные данные клиентов, будет являться процессором данных, а сотрудник - контроллером;
* персональные данные — это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъект данных), по которой прямо или косвенно можно его определить (имя, данные о местоположении, онлайн идентификаторы, IP адрема и т.д.);
* принципы обработки ПД по GDPR
* *законность, справедливость и прозрачность*. ПД должны обрабатываться законно, справедливо и прозрачно. Любую информацию о целях, методах и объёмах обработки ПД следует излагать максимально доступно и просто;
* *ограничение цели*. ПД должны собираться и использоваться исключительно в тех целях, которые заявлены компанией;
* *минимизация данных*. Нельзя собирать ПД в большем объёме, чем это необходимо для целей обработки;
* *точность*. ПД, которые являются неточными, должны быть удалены или исправлены (по требованию пользователя);
* *ограничение хранения*. ПД должны храниться в форме, которая позволяет идентифицировать субъекты ПД на срок не более, чем это необходимо для целей обработки;
* *целостность и конфиденциальность*. При обработке ПД пользователей компании обязаны обеспечить защиту персональных данных от несанкционированной или незаконной обработки, уничтожения и повреждения.
* каждое государство ЕС на законодательном уровне создает надзорный орган Data Protect Authorities (DPA)., функцией которого в том числе будет и рассмотрение вопроса о наложении штрафов за нарушение GDPR. Штрафы – 20 млн евро или 4% от годового дохода компании, причем выбирается большая из сумм;
* уведомление о случаях нарушения GDPR. Организации обязаны уведомлять надзорные органы Data Protect Authorities – DPA, а также субъектов ПД о любых нарушениях, связанных с ПД в течение 72 часов после обнаружения такого нарушения;
* права субъектов по контролю за их ПД. Субъекты имеют право запрашивать подтверждение факта обработки их ПД, место и цель обработки, категории обрабатываемых ПД, каким третьим лицам ПД раскрываются, период, в течение которого ПД будут обрабатываться, а также уточнять источник их получения и требовать их исправления. Также субъект имеет право требовать прекращения обработки своих ПД;
* право на забвение (right to erasure, right to be forgotten), которое дает субъекту возможность удалять свои личные данные по запросу во избежание их распространения или передачи третьим лицам;
* право на переносимость ПД (right to data portability). Данное право заключается в том, что организации обязаны предоставлять бесплатно электронную копию ПД другой организации по требованию самого субъекта ПД;
* согласие на обработку ПД. Согласие человека на обработку его ПД должно быть выражено в форме утверждения или в форме четких активных действий пользователя. Согласие на обработку персональных данных будет недействительно, если у пользователя не было выбора или не было возможности отозвать свое согласие без ущерба для самого себя. Если пользователь дал согласие на обработку своих ПД, контроллер должен иметь возможность продемонстрировать его;
* защита ПД детей. Согласие на обработку данных ребенка должно быть авторизовано родителями (или законными представителями ребенка). Возрастной порог для родительской авторизации устанавливается государствами-членами ЕС отдельно (от 13 до 16 лет);
* назначение уполномоченного по защите ПД (Data Protection Officer). Это требование относится к организациям, которые осуществляют регулярные и систематические наблюдения, мониторинг лиц или которые осуществляют обработку специальных персональных данных, например, медицинские записи или сведения об уголовной судимости;
* источники ПД:
* *предоставленные данные* – данные, полученные от субъектов или их представителей, например, заполнение веб-форм на сайте, представление интересов в суде;
* *распространенные данные* – данные, взятые из общедоступных или открытых источников, например, исследование учетных записей в социальных сетях;
* *наблюдаемые данные* – данные, зафиксированные путем отслеживания действий, например, онлайн-трекинг, геолокация, видеонаблюдение;
* *принятые данные* – данные, полученные не от субъектов, а от других лиц, например, рекомендация от бывшего работодателя соискателя;
* *назначенные данные* – данные, временно или постоянно присвоенные субъектам, например, номер социального страхования, наименование должности;
* *производные данные* – данные, созданные путем простого анализа других данных, например, расчет прибыльности клиента по количеству посещений и купленных товаров;
* *предполагаемые данные* – данные, созданные путем анализа корреляции между наборами данных, например, расчет кредитного рейтинга или прогнозирование состояния здоровья
* на что обратить внимание:
* оценка сбалансированности законных интересов субъекта и контроллера;
* предоставляемая информация при сборе ПД;
* право на удаление данных («право на забвение»);
* право на переносимость данных;
* автоматизированное индивидуальное принятие решений, включая составление профиля;
* защита ПД по умолчанию;
* защита ПД на основе продуманных действий;
* действия представителей контролёров или обработчиков, не учрежденных в Евросоюзе;
* уведомление надзорного органа об утечке ПД;
* сообщение субъекту ПД об утечке его ПД;
* оценка воздействия на защиту ПД;
* назначение на должность инспектора по защите ПД;
* сертификация технических средств, используемых при защите ПД;
* сотрудничество между руководящим надзорным органом и заинтересованными надзорными органами («механизм единого окна»)
* права субъектов ПД:
* право на защиту ПД;
* право распоряжаться своими ПД;
* право в любое время отозвать согласие на обработку ПД;
* право на информацию и транспарентность в отношении обработки ПД;
* право на доступ к ПД;
* право на внесение исправлений в ПД;
* право на удаление ПД;
* право на ограничение обработки ПД;
* право на переносимость ПД;
* право на возражение против обработки ПД;
* право не подчиняться решению, основанному на автоматизированной обработке ПД;
* право быть уведомленным об утечке ПД;
* право на обращение к Data Protection Officer;
* право на обращение (подачу жалобы) к надзорному органу;
* право на эффективные средства судебной защиты против надзорного органа;
* право на эффективные средства судебной защиты в отношении контролёра или обработчика ПД;
* право на представительство (передачу полномочий);
* право на компенсацию материального или нематериального ущерба

***Коммерческая тайна на предприятии***

*Режим КТ обычно создается для достижения следующих целей:*

* создание положительного имиджа организации в случаях взаимоотношений с иностранными организациями, которые привыкли работать в условиях режима КТ;
* решение вышестоящей организации (особенно в госкорпорациях и холдингах);
* защита информации при научных (творческих) разработках до оформления на нее патента (авторских прав);
* выстраивание гражданско-правовых отношений с организациями, имеющими режим КТ (особенно в случаях передачи конфиденциальной информации);
* возможность участвовать в торгах (конкурсах), организованных государственными органами или госкорпорациями, где наличие режима КТ является обязательным условием;
* возможность привлекать работников к юридической ответственности за разглашение информации;
* усложнение получения информации государственными контролирующими и правоохранительными органами;
* рекламные цели (например, контролируемая утечка информации, составляющей КТ);
* увеличение стоимости компании;
* получение прибыли (передача прав использования КТ на основе лицензионного соглашения);
* оправданность траты денег и иных ресурсов на закупку и использование средств защиты информации

*Нормативные документы по КТ*

* Федеральный закон «О коммерческой тайне»;
* Гражданский кодекс РФ;
* Трудовой кодекс РФ

*В Федеральном законе «О коммерческой тайне»* определено:

* КТ должна иметь действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
* требования закона распространяются на информацию, составляющую КТ, независимо от вида носителя, на котором она зафиксирована;
* КТ - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
* информация, составляющая КТ, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим КТ;
* обладатель информации, составляющей КТ, - лицо, которое владеет информацией, составляющей КТ, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим КТ;
* обладателем информации, составляющей КТ, полученную в рамках трудовых отношений, является работодатель;
* разглашение информации, составляющей КТ - действие или бездействие, в результате которых информация, составляющая КТ, 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;
* информация, представляющая КТ должна быть зафиксирована на материальном носителе;
* существуют законные способы получения КТ (например, на основании договора о лицензионном соглашении);
* сведения, которые не могут являться КТ. Можно выделить несколько групп таких сведений:
* содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
* содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
* о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
* о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
* о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;
* о задолженности работодателей по выплате заработной платы и социальным выплатам;
* о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;
* об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
* о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
* о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
* обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.
* взаимоотношения с государственными органами по КТ:
* обладатель информации, составляющей КТ, по мотивированному требованию органа государственной власти предоставляет им на безвозмездной основе информацию, составляющую КТ. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей КТ, и срок предоставления этой информации, если иное не установлено федеральными законами;
* органы государственной власти обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или ИП;
* должностные лица органов государственной власти, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей КТ, не вправе разглашать или передавать другим лицам, органам государственной власти ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую КТ, а также не вправе использовать эту информацию в корыстных или иных личных целях;
* в случае нарушения конфиденциальности информации должностными лицами органов государственной власти, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством РФ;
* в случае отказа обладателя информации, составляющей КТ, предоставить ее органу государственной власти данные органы вправе затребовать эту информацию в судебном порядке;
* обладатель информации, составляющей КТ, а также органы государственной власти, получившие такую информацию, обязаны предоставить эту информацию по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве
* обладатель информации, составляющей КТ, имеет право:
* устанавливать, изменять, отменять в письменной форме режим КТ;
* использовать информацию, составляющую КТ, для собственных нужд;
* разрешать или запрещать доступ к информации, составляющей КТ, определять порядок и условия доступа к этой информации;
* требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей КТ, органов государственной власти, которым предоставлена информация, составляющая КТ, соблюдения обязанностей по охране ее конфиденциальности;
* требовать от лиц, получивших доступ к информации, составляющей КТ, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;
* защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей КТ, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.
* меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя (обязательные требования):
* определение перечня информации, составляющей КТ;
* ограничение доступа к информации, составляющей КТ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
* учет лиц, получивших доступ к информации, составляющей КТ, и (или) лиц, которым такая информация была предоставлена или передана;
* регулирование отношений по использованию информации, составляющей КТ, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
* нанесение на материальные носители, содержащие информацию, составляющую КТ, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).
* наряду с этими мерами обладатель информации, составляющей КТ, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие, не противоречащие законодательству РФ меры;
* меры по охране конфиденциальности информации признаются разумно достаточными, если:
* исключается доступ к информации, составляющей КТ, любых лиц без согласия ее обладателя;
* обеспечивается возможность использования информации, составляющей КТ, работниками и передачи ее контрагентам без нарушения режима КТ.
* в целях охраны конфиденциальности информации работодатель обязан:
* ознакомить под расписку работника, доступ которого к информации, составляющей КТ, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей КТ, обладателями которой является работодатель и его контрагенты;
* ознакомить под расписку работника с установленным работодателем режимом КТ и с мерами ответственности за его нарушение;
* обучить работников правилам работы с информацией, составляющей КТ с подтверждением знаний (зачеты);
* создать работнику необходимые условия для соблюдения им установленного работодателем режима КТ.
* доступ работника к информации, составляющей КТ, осуществляется с его согласия, если иное не предусмотрено его трудовыми обязанностями. Также работник должен взять на себя обязательство по сохранению КТ работодателя;
* в целях охраны конфиденциальности информации, составляющей КТ, работник обязан:
* выполнять установленный работодателем режим КТ;
* не разглашать КТ, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима КТ, в том числе после прекращения действия трудового договора;
* возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей КТ и ставшей ему известной в связи с исполнением им трудовых обязанностей;
* передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую КТ.
* работодатель вправе потребовать возмещения убытков, причиненных ему разглашением КТ, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима КТ;
* ответственность за разглашения информации, составляющей КТ:
* нарушение закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ;
* лицо, которое использовало информацию, составляющую КТ, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может быть привлечено к ответственности. По требованию обладателя информации, составляющей КТ, это лицо обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей КТ, вправе требовать в судебном порядке защиты своих прав;
* причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение КТ, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы
* работник имеет право обжаловать в судебном порядке незаконное установление режима КТ в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей;
* трудовым договором с руководителем организации должны предусматриваться его обязательства по обеспечению охраны конфиденциальности информации, обладателем которой является организация и ее контрагенты, и ответственность за обеспечение охраны ее конфиденциальности;
* отношения между обладателем информации, составляющей КТ, и его контрагентом в части, касающейся охраны конфиденциальности информации, регулируются законом и договором.

*Обычно к КТ рекомендуется отнести следующее:*

* сведения о производстве;
* технологии;
* информация управленческого характера;
* плановые документы;
* финансовые сведения;
* аналитические материалы по рынкам;
* сведения о партнерах и контрагентах;
* информация о переговорах и договоренностях;
* условия договоров;
* ценовая политика.

*Меры по защите КТ:*

* правовые меры;
* организационные меры;
* технические меры;
* кадровые меры

*Что желательно учитывать при создании режима КТ:*

* КТ работодатель не обязан создавать. Это его право, а не обязанность;
* определить процедуры предоставления КТ акционерам;
* в последнее время участились случаи введения режима КТ для защиты от адвокатов;
* подсчитать финансовые затраты при введении режима КТ (экономическая составляющая);
* просчитать организационные затраты при введении режима КТ (удобство работы, быстрота принятия решения и т.д.);
* продумать механизм «допуска» работника к КТ;
* желательно определить время, на которое конкретный документ (конкретная информация) вводится в режим КТ;
* режим КТ является индивидуальным, нет стандартов. Поэтому режимы КТ различаются в разных организациях. В законе предусмотрен только перечень минимальных мероприятий, который должен сделать руководитель, чтобы сказать, что в его организации есть режим КТ;
* если потребуется привлечь работника к ответственности за нарушение режима КТ или за разглашение КТ, то работодателю потребуется доказать, что он сделал тот минимальный набор действий, предусмотренных законом, при создании режима КТ;
* умышленное разглашение работниками КТ может происходить следующими способами:
* разбивание документа на части или размещая их части на внешних серверах и высылая пароли доступа к ним;
* запоминание какой-либо коммерческой информации и дальнейшем ее пересказе заказчикам, без нарушения прав доступа к информации, выносом документов с территории и т.д.;
* при гражданско-правовых отношениях лучше прописывать в самом договоре требования к контрагенту по конфиденциальности информации;
* желательно разделить информацию, составляющую КТ, на группы конфиденциальности и определить по каждой группе свои правила работы с документами;
* утвердить перечень должностей, имеющих доступ к документам, составляющим КТ с указанием конкретных пунктов перечня информации, составляющей КТ, к которым они имеют доступ;
* обязанность сохранять КТ предусмотреть в трудовых договорах всех работников, даже если они не будут иметь к ней доступ;
* создание режима КТ влечет за собой создание конфиденциального делопроизводства;
* привлечь к ответственности за нарушение режима КТ или за разглашение КТ можно только работника, который взял на себя обязательство о сохранении КТ и только за ту КТ, которая стала известна работнику в связи с исполнением им трудовых функций;
* предъявление претензии работнику о разглашении КТ возможно только в период, когда данная информация относилась к КТ;
* на усмотрение руководителя остается вопрос о дополнительном вознаграждении работника за доступ к КТ;
* суды признают вину работника за разглашение КТ только в форме умышленных действиях;
* в законодательстве не определены процедуры доступа и требования по конфиденциальности КТ в судах;
* при гражданско-правовых отношениях лучше прописывать штрафные санкции, а не привязываться к компенсации ущерба, так как возникнут сложности с оценкой стоимости ущерба;
* суды могут трактовать следующее – к КТ работодатель может отнести только ту информацию, которая имеет реальную стоимость и привлекать к ответственности за разглашение КТ можно только в том случае, если работодатель может подсчитать конкретную сумму убытков в связи с разглашением КТ, то есть надо доказать коммерческую ценность информации;
* один из сдожно реализуемых задач при создании режима КТ - определять в каких документах содержится КТ;
* определить процедуры снятия грифа КТ с документов;
* определить периодичность пересмотра перечня информации, относимой к КТ;
* закон разработан под КТ, зафиксированную на бумажном носителе и сложно реализуется под КТ, зафиксированную на электронных носителях информации

*Что желательно сделать помимо требований, установленных законом «О коммерческой тайне»*

* применять организационные способы защиты информации (например, оптимизировать информационные потоки, разбить КТ на части, хранить КТ на внешних носителях информации и обрабатывать на локальных компьютерах);
* предусмотреть ситуации с разглашением информации, составляющую КТ в кодексах этики и корпоративного поведения;
* оценить надежность работников (их мотивацию), допущенных к работе с информацией, составляющей КТ;
* определить процедуры выноса документов с грифом КТ с территории предприятия и удаленный доступ к документам КТ;
* определить технические и ИТ мероприятия по защите КТ;
* использовать систему шифрования и DLP;
* определить процедуры проведения внутренних расследований по фактам разглашения КТ или нарушения режима КТ;
* определить процедуры передачи КТ государственным органам;
* определить процедуры оценки конфиденциальности информации, передаваемой в СМИ, контрагентам и размещаемой в Интернете;
* создать подробную нормативную базу, определяющую правила работы с информацией, составляющей КТ;
* создать пропускной режим на предприятии;
* защитить помещения, в которых будут обрабатываться КТ;
* распределить зоны компетенции между подразделениями по режиму КТ;
* установить системы видеонаблюдения в помещениях, в которых обрабатывается КТ;
* определить - как будет осуществляться контроль за соблюдением режима КТ

*Гражданский кодекс Российской Федерации*

Статья 1465 ГК РФ определяет, что секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны.

Законные способы получения КТ:

* на основании лицензионного договора или договора об отчуждении исключительного права (ст.1468 и 1469 ГК РФ);
* полученной организацией добросовестным и независимым путем (ст. 1466 ГК РФ)

*Трудовой кодекс Российской Федерации (статья 57)*

### В статье 57 ТК определено, что в трудовом договоре могут предусматриваться условия о неразглашении охраняемой законом тайны - государственной, служебной, коммерческой и иной.

Необходимо помнить, что по законодательству РФустановлены специальные случаи прекращения права на КТ, например, с момента принятия арбитражным судом решения о признании должника банкротом сведения о финансовом состоянии должника прекращают относиться к категории сведений, носящих конфиденциальный характер либо являющихся КТ (ФЗ "О несостоятельности (банкротстве)"), с момента вынесения арбитражным судом решения о ликвидации кредитной организации сведения о финансовом состоянии кредитной организации перестают быть отнесенными к категории сведений, носящих конфиденциальный характер либо являющихся КТ (ФЗ «О банках и банковской деятельности»).

*Признаки и особенности коммерческой тайны:*

* коммерческая ценность;
* недоступность;
* охраняемость;
* не требует государственной регистрации права;
* срок конфиденциальности определяется владельцем

*Методы определения КТ на предприятии:*

* *тотальный -* сущность этого метода заключается в том, что КТ на предприятии признается все, за исключением информации, которая не может являться КТ по закону. Этот способ наиболее прост и наименее эффективен, так как реализация мер по защите КТ, определенной таким способом, будет затруднительна и мешать бизнес процессам;
* *плагиаторский* - данный метод основан на том, что необходимо выяснить, какую именно информацию аналогичные профильные компании считают КТ и поступить так же. Претворение данного способа в жизнь, как правило, затрудняется тем, что при определении КТ очень мало универсальных положений, которые подходят абсолютно всем;
* *аналитический* - анализ, какая именно информация могла бы заинтересовать конкурентов или недоброжелателей и разглашение какой информации принесет предприятию убытки;
* *экспертный* – приглашение независимых экспертов. Наиболее эффективный, но и самый дорогостоящий метод

*Ответственность за разглашение КТ*

*Ответственность за разглашение КТ или нарушение режима КТ:*

* уголовная ответственность в разрезе статей УК РФ, связанной с разглашением КТ;
* административная ответственность в разрезе «недобросовестная конкуренция» (компетенция ФАС;
* административная ответственность в разрезе нарушения законодательства о персональных данных (компетенция Роскомнадзора);
* дисциплинарная ответственность за разглашение КТ или нарушение режима КТ;
* материальная ответственность работника (при наличии ущерба);
* имущественная ответственность;
* гражданско-правовая ответственность при наличии интеллектуальной собственности, исключительных прав и т.д.;
* общественное порицание (нарушение кодекса этики)

*Уголовная ответственность*

* *в части первой статьи 183 УК РФ* определено, что собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом - наказывается штрафом в размере до 500 000 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.

Для наступления уголовной ответственности достаточно самого факта собира­ния сведений, составляющих коммерческую или служебную тайну, независимо от наступления вредных последствий.

* *в части второй статьи 183 УК РФ* определено, что 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 1 000 000 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 3 лет, либо исправительными работами на срок до 2 лет, либо принудительными работами на срок до 3 лет, либо лишением свободы на тот же срок.
* *в части третьей статьи 183 УК РФ* определено, что те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются штрафом в размере до 1 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок.
* *в части четвертой статьи 183 УК РФ* определено, что деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, - наказываются принудительными работами на срок до 5 лет либо лишением свободы на срок до 7 лет

*Дисциплинарная ответственность*

* *в статье 81 ТК РФ* предусмотрено расторжение трудового договора по инициативе работодателя в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей;
* в соответствии с ТК РФ за нарушение установленных правил работы (в том числе с КТ) может быть наложено одно из дисциплинарных взысканий (замечание или выговор)

*Имущественная ответственность*

Статья 1472 ГК РФ определяет, что нарушитель исключительного права на секрет производства, в том числе лицо, которое неправомерно получило сведения, составляющие секрет производства, и разгласило или использовало эти сведения, а также лицо, обязанное сохранять конфиденциальность секрета производства, *обязано возместить убытки*, причиненные нарушением исключительного права на секрет производства, если иная ответственность не предусмотрена законом или договором с этим лицом.

Возмещение убытков в полном объеме в соответствии с ГК РФ: убытки = реальный ущерб + упущенная выгода, где: реальный ущерб = фактически понесенные расходы на восстановление нарушенного права + расходы, которые лицо должно будет произвести для восстановления нарушенного права + утрата или повреждение имущества; упущенная выгода = неполученные доходы, которые лицо получило бы, если бы его права не были нарушены. Отметим, что при разглашении информации, составляющей КТ, у ее обладателя отсутствует утрата или повреждение имущества, поскольку такая информация имуществом не является. Если лицо отказывается возместить убытки в добровольном порядке, то обладатель информации, чьи права нарушены, может обратиться в суд. При этом лицу, требующему возмещения, нужно будет позаботиться о подтверждении размеров таких расходов обоснованным расчетом. Срок исковой давности для взыс­кания убытков в данном случае составляет 3 года и начинает исчисляться со дня, когда лицо узнало или должно было узнать о нарушении своего права.

При этом ущерб должен быть возмещен независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

Работник и лица, прекратившие трудовые обязанности с данным работодателем, освобождаются от возмещения причиненного ущерба или убытков в случаях, если разглашение информации, составляющей КТ, явилось следствием непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств (природных катаклизмов, крайней необходимости, то есть невозможности применения иных средств для устранения опасности, непосредственно угрожающей личности, охраняемым законом интересам общества или государства или неисполнения работодателем обязанности по обеспечению режима КТ.

* в соответствии со статьей 238 ТК РФ работник обязан возместить работодателю причиненный ему прямой действительный ущерб (в том числе и при разглашении КТ). Неполученные доходы (упущенная выгода) взысканию с работника не подлежат;
* в статье 243 ТК РФ предусмотрена материальная ответственность в полном размере причиненного ущерба при разглашении сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную) в случаях, предусмотренных федеральными законами.

Однако следует помнить, что если информация, составляющая коммерческую тайну, попала к работнику случайно или по халатности другого работника, который не предупредил о ее ценности, то привлечь к ответственности этого работника нельзя.

*Другие виды ответственности, связанные с нарушением информационной безопасности*

* *статья 138 УК РФ* определяет ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (в том числе деяние, совершенное лицом с использованием своего служебного положения);
* *статья 138.1 УК РФ* определяет ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации;
* *статья 272 УК РФ* предусматривает ответственность за неправомерный доступ к компьютерной информации;
* *статья 273 УК РФ* предусматривает ответственность за создание, использование и распространение вредоносных компьютерных программ;
* *статья 274 УК РФ* предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
* *статья 185.6. УК РФ* предусматривает ответственность за неправомерное использование инсайдерской информации

**Противодействие неправомерному использованию инсайдерской информации**

* инсайдерская информация - точная и конкретная информация, которая не была распространена (в том числе [сведения](consultantplus://offline/ref=17507915D2420F5AD9F72C53E0D9F3D6F5D4F9549A9FD90A6F254562EA1D3E4324F61182176A4757EFE5C98DM4vDD), составляющие коммерческую, служебную, банковскую тайну, тайну связи и иную охраняемую законом тайну) и распространение которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров;
* манипулирование рынком - *умышленные* действия, которые определены законодательством РФ о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком или нормативными актами Банка России, в результате которых цена, спрос, предложение или объем торгов финансовым инструментом, иностранной валютой и (или) товаром отклонились от уровня или поддерживались на уровне, существенно отличающемся от того уровня, который сформировался бы без таких действий;
* инсайдеры могут быть как юридические, так и физические лица. К ним относятся:
* эмитенты (организации, выпускающие ценные бумаги, например, акции), в том числе иностранные эмитенты, и управляющие компании;
* организаторы торговли (например, биржи), клиринговые организации, а также депозитарии и кредитные организации, осуществляющие расчеты по результатам сделок, совершенных через организаторов торговли;
* профессиональные участники рынка ценных бумаг (например, брокеры) и иные лица, осуществляющие в интересах клиентов операции с финансовыми инструментами, иностранной валютой и (или) товарами, получившие инсайдерскую информацию от клиентов;
* лица, имеющие доступ к инсайдерской информации на основании договоров, (например, аудиторские организации, оценщики, кредитные организации, страховые организации);
* лица, которые имеют право прямо или косвенно (через подконтрольных им лиц) распоряжаться не менее чем 25 процентами голосов в высшем органе управления инсайдера - юридического лица, а также лица, которые в силу владения акциями (долями) в уставном капитале, имеют доступ к инсайдерской информации на основании федеральных законов, учредительных документов или внутренних документов;
* члены совета директоров (наблюдательного совета), члены коллегиального исполнительного органа, лицо, осуществляющее функции единоличного исполнительного органа, члены ревизионной комиссии в инсайдере-юридическом лице;
* лица, имеющие доступ к информации о подготовке и (или) направлении добровольного, обязательного или конкурирующего предложения о приобретении ценных бумаг;
* федеральные органы исполнительной власти, исполнительные органы государственной власти субъектов РФ, органы местного самоуправления, органы управления государственных внебюджетных фондов, имеющих в соответствии с российским законодательством право размещать временно свободные средства в финансовые инструменты, публично-правовые компании, Банк России;
* имеющие доступ к инсайдерской информации руководители федеральных органов исполнительной власти, руководители исполнительных органов государственной власти субъектов РФ, выборные должностные лица местного самоуправления, имеющие доступ к инсайдерской информации государственные служащие и муниципальные служащие этих органов;
* информационные агентства, осуществляющие раскрытие информации инсайдеров - юридических лиц;
* лица, осуществляющие присвоение кредитных рейтингов инсайдеров – юридических лиц;
* физические лица, имеющие доступ к инсайдерской информации инсайдеров-юридических лиц, на основании трудовых и (или) гражданско-правовых договоров, заключенных с соответствующими лицами.
* инсайдеры - юридические лица обязаны составлять собственные перечни инсайдерской информации. Собственные перечни инсайдерской информации включают в себя инсайдерскую информацию, перечень которой утверждается нормативным актом Банка России, и инсайдерскую информацию, утверждаемую лицом, осуществляющим функции единоличного исполнительного органа;
* к инсайдерам не относят родственников инсайдеров, но в законодательстве применяется понятие «конфликт интересов», которое распространяется на «иные близкие отношения»;
* инсайдеры – работники должны взять на себя обязательство по сохранении инсайдерской тайны на период ее конфиденциальности. Желательно прописать это в трудовом договоре и в должностных обязанностях;
* доступ работника к инсайдерской тайне должен быть добровольный. Отказ работника от работы с инсайдерской тайной предполагает изменение трудовых обязанностей;
* в инсайдере – юридическом лице может быть проработан вопрос о дополнительной мотивации инсайдеров – работников организации;
* проведение внутренних проверок и расследований в части нарушения правил работы с инсайдерской информацией должно проводиться в соответствии с ТК РФ;
* отдельных правовых требований к лицам, допущенным к работе с инсайдерской информацией в законодательстве нет;
* перечень инсайдерской информации для инсайдеров - юридических лиц определяется Банком России, а также самим юридическим лицом;
* Указанием ЦБ РФ от 21.11.2019 № 5326-У утвержден перечень инсайдерской информации для юридических лиц, а также порядок и сроки ее раскрытия. Некоторая инсайдерская информация не раскрывается;
* к инсайдерской информации на основе требований ЦБ относится:
* *инсайдерская информация эмитента*, эмиссионные ценные бумаги которого допущены к организованным торгам или в отношении эмиссионных ценных бумаг которого подана заявка о допуске к организованным торгам;
* инсайдерская информация управляющей компании;
* инсайдерская информация организатора торговли;
* инсайдерская информация клиринговой организации, а также депозитария и кредитной организации, осуществляющих расчеты по результатам сделок, совершенных через организаторов торговли;
* инсайдерская информация профессионального участника рынка ценных бумаг и иного лица, осуществляющего в интересах клиентов операции с финансовыми инструментами, иностранной валютой и (или) товарами, допущенными к организованным торгам (в отношении которых подана заявка о допуске к организованным торгам), получивших инсайдерскую информацию от клиентов;
* инсайдерская информация информационного агентства, осуществляющего раскрытие информации инсайдеров – юридических лиц;
* инсайдерская информация кредитного рейтингового агентства, осуществляющего рейтинговые действия в отношении инсайдеров – юридических лиц.
* перечни инсайдерской информации инсайдеров - юридических лиц подлежат раскрытию в информационно-телекоммуникационной сети "Интернет" на их официальных сайтах;
* к инсайдерской информации не относятся:
* сведения, ставшие доступными неограниченному кругу лиц, в том числе в результате их распространения;
* осуществленные на основе общедоступной информации исследования, прогнозы и оценки в отношении финансовых инструментов, иностранной валюты и (или) товаров, а также рекомендации и (или) предложения об осуществлении операций с финансовыми инструментами, иностранной валютой и (или) товарами.
* запрещается использование инсайдерской информации:
* для осуществления операций с финансовыми инструментами, иностранной валютой и (или) товарами, которых касается инсайдерская информация, за свой счет или за счет третьего лица;
* путем передачи ее другому лицу, за исключением случаев передачи этой информации лицу, включенному в список инсайдеров, в связи с исполнением обязанностей, установленных федеральными законами, либо в связи с исполнением трудовых обязанностей или исполнением договора;
* путем дачи рекомендаций третьим лицам, обязывания или побуждения их иным образом к приобретению или продаже финансовых инструментов, иностранной валюты и (или) товаров.
* к наиболее распространенным типам инсайдерской информации в публичных акционерных обществах относятся сведения о «финансовом здоровье» или стабильности компании (доходы, прибыли, случаи банкротства и т.д.), об изменениях в структуре компании в результате слияний, поглощения или создания новых предприятий, а также о новых продуктах, технологиях, лицензиях и пр;
* инсайдерская информация должна быть документирована (зафиксирована в документах) или в проектах документов;
* инсайдерская информация может быть «своя» (в соответствии с перечнем инсайдерской информации, утвержденной приказом организации) и может быть «чужая», то есть полученная от других организаций;
* понятие «инсайд» и «инсайдерская информация» может применяться как в юридическом контексте ФЗ – 224, так и в бытовом (сленговом) контексте, то есть это вся внутренняя информация, которая доступна работникам, в том числе в виде слухов;
* в инсайдерскую информацию может входить иная, охраняемая законом тайна (коммерческая тайна, служебная тайна, персональные данные и т.д.). Не урегулирован вопрос приоритетов правовых режимов в случае, если инсайдерская информация относится к коммерческой тайне;
* на документах, содержащих инсайдерскую информацию нет ограничительного грифа или ограничительной пометки;
* инсайдерская информация имеет срок конфиденциальности, после которого она обязана раскрываться. Срок конфиденциальности определяет Банк России и само предприятие;
* по мотивированному требованию инсайдерская информация предоставляется правоохранительным органам, а также по запросам судов;
* неправомерное использование инсайдерской информации в определенных ситуациях будет относиться к коррупционным правонарушениям (использование должностного положения, нарушая закон, и имея при этом выгоду);
* инсайдерская информация должна быть неправомерно использована, а не только разглашена;
* работа с инсайдерской информации предполагает не только работу в правовом поле, но и этичность в действиях инсайдеров – физических лиц;
* нарушение правил работы с инсайдерской информацией может быть умышленной (неправомерное использование и т.д.) и не умышленной (нарушение правил конфиденциальности);
* инсайдерская информация по прошествии определенного количества времени (наступления определенного события) подлежит раскрытию. Но постановлением Правительства РФ утверждены перечни инсайдерской информации, которая может раскрываться в ограниченных составе и (или) объеме;
* порядок и сроки раскрытия инсайдерской информации, перечень которой утверждается нормативным актом Банка России, устанавливаются нормативными актами Банка России;
* порядок и сроки раскрытия инсайдерской информации инсайдеров – юридических лиц определены приказом ФСФР от 28.02.2012 г. № 12-9/пз-н;
* сообщение об инсайдерской информации лиц, являющихся инсайдерами, должно быть опубликовано в следующие сроки с даты наступления соответствующего факта (события, действия) или даты, в которую лицо, являющееся инсайдером, узнало или должно было узнать о его наступлении:
* в ленте новостей информационных агентств - не позднее 1 дня;
* на странице инсайдера – юридического лица в сети Интернет - не позднее 2 дней.
* инсайдеры - юридические лица обязаны:
* вести список инсайдеров;
* уведомлять лиц, включенных в список инсайдеров, об их включении в такой список и исключении из него, информировать указанных лиц о требованиях настоящего законодательства;
* передавать организатору торговли, через которого совершаются операции с финансовыми инструментами, иностранной валютой и (или) товаром, по его требованию в [порядке](consultantplus://offline/ref=17507915D2420F5AD9F72C53E0D9F3D6FFD5F65A9B908400677C4960ED12614631E7498E17755951F7F9CB8F4EM2vBD), установленном нормативным актом Банка России, список инсайдеров;
* передавать список инсайдеров в Банк России по его требованию.
* инсайдеры - юридические лица вправе запросить у инсайдеров, включенных в список инсайдеров, информацию об осуществленных ими операциях с ценными бумагами этого инсайдера-юридического лица и о заключении договоров, которые являются производными финансовыми инструментами и цена которых зависит от таких ценных бумаг;
* порядок доступа к инсайдерской информации и меры по охране ее конфиденциальности определены Методическими рекомендациями, утвержденными Банком России 14.09.2018 N 23-МР;
* инсайдеры - юридические лица обязаны:
* разработать и утвердить порядок доступа к инсайдерской информации, правила охраны ее конфиденциальности и контроля за соблюдением требований законодательства;
* создать (определить, назначить) структурное подразделение (должностное лицо), в обязанности которого входит осуществление контроля за соблюдением требований законодательства и которое подотчетно лицу, осуществляющему функции единоличного исполнительного органа;
* обеспечить условия для беспрепятственного и эффективного осуществления назначенным структурным подразделением (должностным лицом) своих функций.

Международные стандарты в области информационной безопасности ISO 27000

*Международный стандарт* ***ISO 27001*- система управления информационной безопасностью** -ISO 27001:2005 (BS 7799-2:2005) обеспечивает процессы создания, внедрения, применения, мониторинга, анализа, сопровождения и совершенствования с**истемы управления информационной безопасностью** (ISMS). Данный международный стандарт может использоваться для оценки соблюдения требований заинтересованными внутренними и внешними сторонами.

***Международный стандарт ISO 27002* - Практические правила управления информационной безопасностью** (CPISM) является международным стандартом в области управления информационной безопасностью. Он может использоваться как коммерческими, так и некоммерческими организациями на всех уровнях и во всех секторах рынка, независимо от размера организации. Он может использоваться при создании системы управления безопасностью, для анализа состояния и повышения уровня безопасности в организации.

Данный стандарт существует с 2007 года и называется Практические правила менеджмента информационной безопасности. Стандарт предоставляет лучшие практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента информационной безопасности. Текущая версия стандарта состоит из следующих основных разделов:

* политика безопасности (*Security policy*);
* организация информационной безопасности (*Organization of information security*);
* управление ресурсами (*Asset management*);
* безопасность персонала (*Human resources security*);
* физическая безопасность и безопасность окружения (*Physical and environmental security*);
* управление коммуникациями и операциями (*Communications and operations management*);
* управление доступом (Access control);
* приобретение, разработка и поддержка систем (Information systems acquisition, development and maintenance);
* управление инцидентами информационной безопасности (*Information security incident management*);
* управление бесперебойной работой организации (*Business continuity management*);
* соответствие нормативным требованиям (*Compliance*)

*Американская концепция системного подхода к обеспечению защиты конфиденциальной информации (OPSEC Operation Security)*

В американском бизнесе существует универсальная концепция системного подхода к информационной безопасности, которая строится на 7 этапах ее реализации.

*Первый этап* (анализ объекта защиты) состоит в определении - что нужно защищать и проводится по следующим направлениям:

* какая информация нуждается в защите;
* наиболее важные (критические) элементы защищаемой информации;
* срок жизни критической информации (время, необходимое конкуренту для реализации добытых сведений);
* определяются ключевые элементы информации (индикаторы), отражающие характер охраняемых сведений;
* классифицируются индикаторы по функциональным зонам (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения управления и т.д.).

*Второй этап*– осуществляется "выявление угроз". Он происходит по следующим направлениям:

* определяется, кого может заинтересовать защищаемая информация;
* оцениваются методы, используемые конкурентами для получения этой информации;
* оцениваются вероятные каналы утечки информации;
* разрабатывается система мероприятий по пресечению действий конкурента.

*Третий этап* **–** анализируетсяэффективность принятых и постоянно действующих подсистем безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.д.).

*Четвертый этап* – определение необходимых мер защиты. На основании проведенных на первых трех этапах аналитических исследований определяются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.

*Пятый этап* – руководителями предприятия рассматриваются представленные предложения по всем необходимым мерам безопасности и расчет их стоимости и эффективности.

*Шестой этап*– реализация принятых дополнительных мер безопасности с учетом установленных приоритетов.

*Седьмой этап* – осуществление контроля и доведение до персонала реализуемых мер безопасности.

**Конфиденциальное делопроизводство**

*Виды конфиденциальных документов:*

* документ, имеющий реквизит и зафиксированный на материальном носителе (например, бумажном);
* электронный документ, подписанный цифровой подписью;
* электронная копия материального документа

*Угрозы, которым чаще всего подвергаются конфиденциальные документы (конфиденциальная информация):*

* разглашение информации, содержащейся в конфиденциальных документах;
* изменение информации, содержащейся в конфиденциальных документах;
* включение конфиденциальной информации в открытые документы;
* включение в документы избыточной конфиденциальной информации;
* ознакомление избыточно большого количества работников с конфиденциальными документами;
* нарушение установленных правил работы с конфиденциальными документами;
* несанкционированное создание конфиденциальных документов;
* занижение грифа конфиденциальности (при их наличии);
* отсутствие регистрации черновиков, вариантов документа и т.д.

*При создании конфиденциального делопроизводства необходимо ответить на вопросы:*

*Общие вопросы:*

* выбор системы конфиденциального электронного документооборота (СЭД) и совместимость его с общим документооборотом;
* получение и использование цифровой подписи;
* оптимизация информационных потоков с целью минимизации затрат на создание конфиденциального делопроизводства;
* определение, присвоение, снятие и пересмотр грифа конфиденциальности;
* должностное лицо (подразделение), которое отвечает за конфиденциальное делопроизводство и подчиненность (кураторство);
* порядок учета конфиденциальных документов (ведение реестра), а также учет их перемещения;
* определение перечня документов (кроме конфиденциальных), включаемые в систему конфиденциального делопроизводства;
* оценка конфиденциальности информации в документах, передаваемых в СМИ, размещаемых в Интернете и рекламных материалах;
* доступа к конфиденциальным документам представителей государственных органов;
* порядок контроля и проверки конфиденциального делопроизводства;
* нормативное обеспечение конфиденциального делопроизводства.

*Процедурные вопросы:*

* порядок создания конфиденциальных документов;
* порядок ведения черновых записей, содержащих конфиденциальную информацию;
* порядок уничтожения конфиденциальных документов;
* контроль за исполнением конфиденциальных документов;
* порядок пользования конфиденциальными документами;
* порядок приема-передачи конфиденциальных документов;
* порядок размножения (копирования) конфиденциальных документов;
* порядок печати конфиденциальных документов;
* порядок регистрации и индексации конфиденциальных документов;
* порядок архивного хранения;
* порядок заполнения карточки конфиденциальности документа;
* порядок учета ознакомления с конфиденциальными документами;
* порядок ведения конфиденциальных документов в актуальном состоянии (при необходимости);
* порядок отправки конфиденциальных документов в другие организации;
* порядок доклада руководству и утверждения конфиденциальных документов;
* участие секретарей и секретариата в работе с конфиденциальными документами;
* осуществление выписок из конфиденциальных документов;
* порядок формирования дел с конфиденциальными документами;
* порядок выноса конфиденциальных документов с контролируемой территории;
* порядок работы с конфиденциальными документами за пределами контролируемой территории (командировка, дом и т.д.);
* контроль за конфиденциальным делопроизводством;
* порядок перемещения конфиденциальных документов между территориально удаленными объектами предприятия;
* хранение дубликатов ключей, вскрытия сейфов, опечатывания;
* порядок изменение систем безопасности при компрометации (утеря ключей, печатей и т.д.)

*Инженерно-технические вопросы:*

* оборудование помещений средствами контроля и управления доступом;
* противопожарная защита помещений;
* физическая сохранность конфиденциальных документов в помещениях.

*Вопросы IT безопасности*

* техническая защита электронных документов;
* порядок применения цифровых подписей;
* разграничение доступа и идентификация пользователей;
* удаленный доступ к ЭДО;
* регистрация инцидентов с электронными документами;
* работа с беспроводной связью;
* использование личных гаджетов;
* применение средства криптографической защиты информации;
* расположение сервера и применение облачных хранилищ;
* резервное копирование электронных документов;
* антивирусная защита и защита от несанкционированного доступа;
* применение DLP систем

*Кадровые вопросы:*

* перечень работников (должностей), имеющих доступ к конфиденциальным документам;
* обязательство работника о сохранении конфиденциальной информации;
* проверки работников, допущенных к конфиденциальным документам;
* оценка мотивации и лояльности персонала, работающего с конфиденциальными документами;
* обеспечение работников условиями для работы с конфиденциальными документами;
* психологическая и иная готовность работников к работе с электронными конфиденциальными документами;
* обучение и инструктаж персонала, работающего с конфиденциальными документами;
* порядок оформления разрешения (допуска) на работу с конфиденциальными документами;
* превентивные кадровые мероприятия, направленные на недопущение разглашения конфиденциальной информации;
* порядок проведения внутренних расследований (проверок) по фактам разглашения конфиденциальной информации

*Материально-технические вопросы:*

* технические средства СЭД;
* технические средства для работы с материальными конфиденциальными документами (сейфы, шредеры и т.д.)

*При создании конфиденциального делопроизводства следует иметь в виду*

* не существует стандартов (ГОСТов) по конфиденциальному делопроизводству. Есть стандарт по открытому делопроизводству и требования по секретному делопроизводству. Как правило, конфиденциальное делопроизводство создается на основе обычного делопроизводства, включая в него элементы конфиденциальности

*В соответствии с Инструкцией о порядке обращения с документированной служебной информацией ограниченного распространения в организациях, учреждениях, предприятиях и т.д., утвержденной Главгосэкспертизой России в 2000 году для служебной информации с грифом «Для служебного пользования» предусмотрено:*

* общие положения
* необходимость присвоения документам грифа "ДСП" определяется исполнителем и должностным лицом, подписывающим или утверждающим документ, в соответствии с "Перечнем видов служебной информации, которую необходимо относить к разряду ограниченного распространения", утверждаемой руководителем организации;
* документированная служебная информация ограниченного распространения без санкции руководителя организации или его заместителей не подлежит разглашению (распространению);
* контроль за осуществлением учета, размножения, хранения и использования документов с грифом «ДСП» возлагается на канцелярии или другие подразделения, выполняющие такие функции (общие отделы, секретариаты и т.п.);
* сотрудники организаций, имеющие отношение к работе с документами «ДСП», должны быть в обязательном порядке ознакомлены с инструкцией, устанавливающей порядок работы с документированной информацией ограниченного распространения в организации;
* сотрудникам, работающим с документами «ДСП», запрещается сообщать устно или письменно кому бы то ни было сведения, содержащиеся в этих документах, если это не вызывается служебной необходимостью.
* порядок приема и учета документов «ДСП»
* прием и учет (регистрация) документов «ДСП» осуществляется теми же структурными подразделениями организации, которым поручен учет несекретной документации;
* в случае отсутствия в конвертах (пакетах) документов «ДСП» или приложений к ним составляется акт в двух экземплярах, один из которых высылается отправителю;
* в нерабочее время документы «ДСП» принимаются дежурными по организации, которые, не вскрывая эту корреспонденцию, передают ее работникам службы документационного обеспечения;
* запрещается доставлять в нерабочее время материалы «ДСП» в организации, не имеющие постоянных дежурных;
* регистрации подлежат все входящие, исходящие и внутренние документы, а также издания «ДСП». Такие документы учитываются по количеству листов, а издания (книги, журналы, брошюры) - по экземплярам;
* документы «ДСП» учитываются отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. При этом в карточке (журнале) к регистрационному номеру документа проставляется отметка «ДСП»;
* учет документов «ДСП» ведется на карточках или в журналах. Допускается регистрировать документы «ДСП» с помощью устройств электронно-вычислительной техники;
* на каждом зарегистрированном документе «ДСП» проставляется штамп, в котором указываются наименование организации, регистрационный номер документа и дата его поступления;
* дополнительно размноженные экземпляры документа учитываются за номером этого документа, о чем делается отметка на размножаемом документе и в учетных формах.
* размножение и рассылка (отправка) документов «ДСП»
* документы «ДСП» печатаются специалистом службы документационного обеспечения организации (управление делами, общий отдел, канцелярия и т.п.), ответственным за подготовку документов «ДСП», допускается использование персональной компьютерной техники, при этом работа выполняется только с использованием сменных носителей информации. Указанные носители хранятся у специалиста, ответственного за работу с документами «ДСП»;
* документы «ДСП» печатаются с указанием на лицевой или оборотной стороне в левом нижнем углу последнего листа каждого экземпляра документа количества отпечатанных экземпляров, фамилии исполнителя и номера его служебного телефона. Указываются также наименование файла, дата печатания, инициалы имени и фамилии специалиста, печатавшего документ. Подписанные документы (вместе с черновиками) передаются для регистрации специалисту службы документационного обеспечения организации, осуществляющему их учет;
* документы «ДСП» передаются специалистам структурных подразделений организации под расписку. Передача документов "ДСП" и дел, содержащих такие документы от одного специалиста другому, осуществляется только с разрешения руководителя структурного подразделения организации;
* документы «ДСП» пересылаются сторонним организациям фельдъегерской службой, спецсвязью или заказными или ценными почтовыми отправлениями;
* документы «ДСП» не могут передаваться по незащищенным каналам связи;
* отпечатанные и подписанные документы «ДСП» вместе с их черновиками и вариантами передаются для регистрации специалисту, осуществляющему их учет. Черновики и варианты уничтожаются этим сотрудником с подтверждением факта уничтожения записью на копии исходящего документа: "Черновик (и варианты) уничтожены. Дата. Подпись";
* на исходящих документах (в необходимых случаях и на их проектах), содержащих документированную служебную информацию ограниченного распространения, гриф «ДСП» и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам;
* размножение документов «ДСП» осуществляется только с письменного разрешения руководства организации и под контролем службы документационного обеспечения организации. Учет размноженных документов осуществляется по экземплярам;
* документы «ДСП», полученные от сторонних организаций, могут быть размножены только с их согласия;
* отправляемые документы "ДСП" должны быть помещены в конверты либо упакованы. Запрещается использовать конверты с прозрачными "окошками" для пересылки этих документов;
* запрещается указывать фамилии и должности руководителей и сотрудников, а также наименования структурных подразделений организации на упаковке документов «ДСП».
* группировка исполненных документов «ДСП» в дела
* документы «ДСП» после исполнения группируются в дела. Порядок их группировки предусматривается номенклатурами дел несекретного делопроизводства;
* документы «ДСП» в зависимости от производственной необходимости допускается группировать в дела отдельно или вместе с другими несекретными документами по одному и тому же вопросу;
* при включении документа «ДСП» в дело с несекретными документами, не имеющими аналогичного грифа, данное дело получает гриф «ДСП» и соответствующее уточнение вносится в номенклатуру дел текущего года;
* по окончании календарного года дело «Документы «ДСП» просматривается экспертной комиссией полистно и, в случае необходимости, принимается решение о перегруппировке документов. Содержащиеся в деле документы постоянного срока хранения группируются в отдельное дело (дела), которое получает самостоятельный заголовок и дополнительно включается в номенклатуру дел
* использование документов, дел и изданий. Снятие с документов грифа «ДСП»
* к работе с делами «ДСП» допускаются имеющие к ним непосредственное отношение должностные лица, а к документам - согласно указаниям, содержащимся в резолюциях руководителей организаций (структурных подразделений);
* категории (должности) работников, допускаемых к работе с документами «ДСП» определяются руководителем организации (структурных подразделений);
* представители других организаций допускаются к ознакомлению и работе с документами «ДСП» с разрешения руководителя организации (структурных подразделений), в ведении которых находятся эти материалы, при наличии письменного запроса тех организаций, в которых они работают, с указанием темы выполняемого задания. Дела и издания «ДСП» выдаются исполнителям и принимаются от них под расписку в "Карточке учета выдаваемых дел и изданий";
* снятие копий, а также производство выписок из документов «ДСП» сотрудниками данной организации производится с разрешения руководителя этой организации (структурного подразделения);
* снятие копий для сторонних организаций с документов «ДСП» производится на основании письменных запросов с разрешения руководителя организации (структурного подразделения), подготовившей эти документы;
* дела постоянного и временного сроков хранения с грифом «ДСП» периодически просматриваются с целью возможного снятия этого грифа;
* решение вопроса о снятии грифа «ДСП» возлагается на создаваемую в установленном порядке специальную комиссию, в состав которой включаются представители службы документационного обеспечения организации, режимно-секретного органа (спецчасти) и руководители структурных подразделений организации;
* решение комиссии оформляется составляемым в произвольной форме актом, который утверждается руководителем организации. В акте перечисляются документы и дела, с которых гриф «ДСП» снимается;
* на обложках дел (первых страницах документов) гриф «ДСП» погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия;
* при снятии грифа «ДСП» на документах, изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.
* отбор документов «ДСП» для хранения и к уничтожению
* проведение экспертизы научной и практической ценности документов «ДСП» рассмотрение и утверждение ее результатов производится в соответствии с требованиями и порядком, установленными для несекретных материалов;
* отобранные к уничтожению документы «ДСП», не имеющие исторической ценности и утратившие практическое значение, могут оформляться отдельным актом или включаться в общий акт вместе с другими отобранными к уничтожению несекретными документами
* обеспечение сохранности документов «ДСП». Проверка их наличия
* документы «ДСП» должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность;
* передача документов «ДСП» другим сотрудникам, производится только через службу документационного обеспечения организации;
* запрещается изъятие из дел или перемещение документов с грифом «ДСП» из одного дела в другое без санкции службы документационного обеспечения или лица, осуществляющего их учет. Обо всех проведенных изъятиях или перемещениях делаются отметки в учетных документах, включая внутренние описи;
* запрещается выносить документы «ДСП» из служебных помещений для работы с ними на дому;
* при смене в организации специалиста, ответственного за учет документов «ДСП» составляется акт приема-сдачи этих документов, который утверждается начальником службы документационного обеспечения организации;
* проверка наличия документов «ДСП» в организации проводится не реже одного раза в год комиссией, назначаемой приказом руководителя организации. В состав комиссии включается специалист, ответственный за учет и хранение этих документов;
* результаты проверок оформляются актом;
* о фактах утраты документов «ДСП», а также разглашения информации, содержащейся в этих документах, ставится в известность руководитель организации и назначается комиссия для расследования обстоятельств утраты или разглашения;
* на утраченные документы «ДСП» составляется акт, на основании которого делаются соответствующие отметки в учетных формах.

*Техническая защита конфиденциальной информации*

*Группы технических средств промышленного шпионажа:*

* средства акустического контроля;
* аппаратура для съема информации с окон;
* специальная звукозаписывающая аппаратура;
* микрофоны различного назначения и исполнения;
* электросетевые подслушивающие устройства;
* приборы для съема информации с телефонной линии связи и сотовых телефонов;
* специальные системы наблюдения и передачи видеоизображений;
* специальные фотоаппараты;
* приборы наблюдения в дневное время и приборы ночного видения;
* специальные средства радиоперехвата и приема ПЭМИН

###### Оптический канал утечки информации реализуется в следующем:

* визуальным наблюдением;
* фото и видеосъемкой;
* использованием видимого и инфракрасного диапазонов для передачи информации от скрыто установленных фото и видеокамер

###### Акустический канал утечки информации реализуется:

* прослушивание разговоров на открытой местности и в помещениях, находясь рядом или используя направленные микрофоны;
* негласная запись разговоров на диктофон;
* прослушивание разговоров с использованием выносных микрофонов;
* снятие акустической информации с оконных стекол с помощью лазера;
* прослушивание разговоров с помощью конструктивно доработанных сотовых телефонов;
* прослушивание разговоров через элементы строительных конструкций (стетоскопы).
* считывание информации с губ.

Акустоэлектрический канал утечки информации (получение информации через звуковые волны с дальнейшей передачей ее через сети электропитания)

Особенности электроакустического канала утечки информации:

* удобство применения (электросеть есть везде);
* постоянное питание у микрофона;
* трансформаторная развязка является препятствием для дальнейшей передачи информации по сети электропитания;
* возможность съема информации с питающей сети, не подключаясь к ней (используя электромагнитное излучение сети электропитания);
* возможные помехи на бытовых приборах при использовании электросети для передачи информации, а также плохое качество передаваемого сигнала при большом количестве работы бытовых приборов.

Телефонный канал утечки информации

Использование телефонного канала утечки информации возможно по следующим направлениям:

* прослушивание телефонных переговоров;
* использование телефонного аппарата для акустического контроля помещения.

*Радиотелефонный канал утечки информации*

При использовании сотового телефона следует знать:

* системы защиты информации, которыми оснащены сотовые телефоны ненадежны и не гарантированы от подслушивания, в связи с чем, не рекомендуется вести конфиденциальные переговоры по сотовой связи;
* у сотовых телефонов имеются «недекларированные возможности», например, сотовый телефон может быть удаленно и негласно активирован без какой либо индикации и без ведома владельца;
* необходимо учитывать, что при включенном сотовом телефоне всегда можно запеленговать и вычислить местоположение абонента;
* при фотографировании сотовым телефоном определяются координаты места фотографирования и можно их прочитать через электронный вариант фотографии.

*Специальные технические средства негласного получения информации могут быть установлены следующими способами:*

* во время строительных или ремонтных работ;
* в предметы мебели, другие предметы интерьера и обихода, в различные технические средства как общего назначения, так и предназначенные для обработки информации;
* в предметы, которые вручаются в качестве подарков, а впоследствии могут использоваться для оформления интерьера служебных помещений;
* в ходе обслуживания помещений и профилактики инженерных сетей. При этом в качестве исполнителя могут быть использованы технические работники

*Приборы обнаружения технических средств промышленного шпионажа*

* устройства поиска активного типа, которые сами воздействуют на объект и анализируют сигнал отклика:
* нелинейные локаторы;
* рентгенометры;
* магнитно-резонансные локаторы;
* акустические корректоры
* устройства поиска пассивного типа:
* металлоискатели;
* тепловизоры;
* устройства поиска по электромагнитному излучению;
* устройства поиска аномальных параметров телефонной линии;
* устройства поиска аномалий магнитного поля.

**Информация об авторе:**

**Панкратьев Вячеслав Вячеславович –** полковник юстиции в запасе, заведующий кафедрой безопасности в Университете государственного и муниципального управления, эксперт в области корпоративной безопасности, защите активов и управлению рисками. Преподаватель - консультант, автор и ведущий обучающих семинаров и курсов повышения квалификации по тематикам, связанных с корпоративной безопасностью. Опыт преподавания и консалтинга с 1997 года. Автор книг и методических пособий по безопасности предпринимательской деятельности. Независимый консультант. Разработчик методик аудита безопасности предприятия и создания КСБ – корпоративных стандартов безопасности.

**www.vvpankrat.ru**

**vv\_pankrat@mail.ru**

**+7-963-632-41-20**