Если компания хранит бухгалтерскую информацию, клиентскую базу, анкеты сотрудников или корпоративные тайны, то важно, чтобы эти данные не попали не в те руки, то есть были защищены. Защитой данных занимается информационная безопасность. Разобрались, что это и какие именно данные она защищает.

## **Что такое информационная безопасность**

Информационная безопасность — это различные меры по защите информации от посторонних лиц. В доцифровую эпоху для защиты информации люди запирали важные документы в сейфы, нанимали охранников и шифровали свои сообщения на бумаге.

Сейчас чаще защищают не бумажную, а цифровую информацию, но меры, по сути, остались теми же: специалисты по информационной безопасности создают защищенные пространства (виртуальные «сейфы»), устанавливают защитное ПО вроде антивирусов («нанимают охранников») и используют криптографические методы для шифрования цифровой информации.

Однако цифровую информацию тоже нужно защищать не только виртуально, но и физически. Антивирус не поможет, если посторонний похитит сам сервер с важными данными. Поэтому их ставят в охраняемые помещения.

## **За что отвечает информационная безопасность**

Она отвечает за три вещи: конфиденциальность, целостность и доступность информации. В концепции информационной безопасности их называют принципами информационной безопасности.

**Конфиденциальность** означает, что доступ к информации есть только у того, кто имеет на это право. Например, ваш пароль от электронной почты знаете только вы, и только вы можете читать свои письма. Если кто-то узнает пароль или другим способом получит доступ в почтовый ящик, конфиденциальность будет нарушена.

**Целостность**означает, что информация сохраняется в полном объеме и не изменяется без ведома владельца. Например, на вашей электронной почте хранятся письма. Если злоумышленник удалит некоторые или изменит текст отдельных писем, то это нарушит целостность.

**Доступность**означает, что тот, кто имеет право на доступ к информации, может ее получить. Например, вы в любой момент можете войти в свою электронную почту. Если хакеры атакуют серверы, почта будет недоступна, это нарушит доступность.

## **Какая бывает информация и как ее защищают**

Информация бывает общедоступная и конфиденциальная. К общедоступной имеет доступ любой человек, к конфиденциальной — только отдельные лица.

Может показаться, что защищать общедоступную информацию не надо. Но на общедоступную информацию не распространяется только принцип конфиденциальности — она должна оставаться целостностной и доступной. Поэтому информационная безопасность занимается и общедоступной информацией.

Например, возьмем интернет-магазин. Карточки товаров, статьи в блоге, контакты продавца — все это общедоступная информация, ее может просматривать любой. Но интернет-магазин все равно нужно защищать, чтобы никто не нарушил его работу, например, не изменил важную информацию в карточках товаров или не «уронил» его сайт.

Главная задача информационной безопасности в IT и не только — защита конфиденциальной информации. Если доступ к ней получит посторонний, это приведет к неприятным последствиям: краже денег, потере прибыли компании, нарушению конституционных прав человека и другим неприятностям.

Если с общедоступной информацией все понятно, то о конфиденциальной информации стоит поговорить отдельно, так как у нее есть несколько разновидностей.

## **Основные виды конфиденциальной информации**

[**Персональные данные**](https://mcs.mail.ru/blog/chto-takoe-personalnye-dannye-ih-hranenie-i-obrabotka)**.** Информация о конкретном человеке: ФИО, паспортные данные, номер телефона, физиологические особенности, семейное положение и другие данные.

Тот, кто работает с персональными данными, обязан защищать их и не передавать третьим лицам. Информация о клиентах и сотрудниках относится как раз к персональным данным.

**Коммерческая тайна.**Внутренняя информация о работе компании: технологиях, методах управления, клиентской базе. Если эти данные станут известны посторонним, компания может потерять прибыль.

Компания сама решает, что считать коммерческой тайной, а что выставлять на всеобщее обозрение. При этом не вся информация может быть коммерческой тайной — например, нельзя скрывать имена учредителей юрлица, условия труда или факты нарушения законов.

**Профессиональная тайна.** Сюда относятся врачебная, нотариальная, адвокатская и другие виды тайны, относящиеся к профессиональной деятельности. С ней связано [сразу несколько законов](http://www.consultant.ru/document/cons_doc_LAW_93980/#dst0).

**Служебная тайна.**Информация, которая известна отдельным службам, например, налоговой или ЗАГСу. Эти данные обычно хранят государственные органы, они отвечают за их защиту и предоставляют только по запросу.

**Государственная тайна.**Сюда относят военные сведения, данные разведки, информацию о состоянии экономики, науки и техники государства, его внешней политики. Эти данные самые конфиденциальные — к безопасности информационных систем, в которых хранится такая информация, предъявляют самые строгие требования.

Если ваша компания хранит персональные данные, коммерческую или профессиональную тайну, то эти данные нужно защищать особым образом. Для этого необходимо ограничить доступ к ней посторонним лицам — установить уровни доступа и пароли, поставить защитное ПО, настроить шифрование.

**1. Основы безопасности данных**

Кратко об информационной безопасности и защите информации

1. Информационная безопасность отвечает за защиту данных и обеспечивает их конфиденциальность, целостность и доступность.
2. Конфиденциальность означает, что доступ к данным есть только у тех, кто имеет на это право.
3. Целостность означает, что данные хранятся в неизменном виде и остаются достоверными.
4. Доступность означает, что человек, у которого есть право на доступ к информации, может ее получить.
5. Информационная безопасность защищает и конфиденциальные, и общедоступные данные. Общедоступным она обеспечивает целостность и доступность, конфиденциальным — еще и нужный уровень секретности.
6. К конфиденциальной информации относятся персональные данные, коммерческая, профессиональная, служебная и государственная тайны.

# **Виды информационных угроз**

Информационные угрозы могут быть обусловлены:

* естественными факторами (пожар, наводнение, и др.);
* человеческими факторами.

Последние, в свою очередь, подразделяются на:

* угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации;
* угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с несанкционированным доступом к ресурсам АИС.

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование (прослушивание).

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы также подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.

Под внутренними угрозами понимаются — угрозы безопасности информации инсайдером (исполнителем) которых является внутренний по отношению к ресурсам организации субъект (инсайдер).

Под внешними угрозами понимаются — угрозы безопасности информации инициатором (исполнителем) которых является внешний по отношению к ресурсам организации субъект (удаленный хакер, злоумышленник).

## Внутренние угрозы

* Утечки информации
* Неавторизованный доступ

## Внешние угрозы

* Вредоносные программы (вирусы, троянцы, черви и т.д.)
* Атаки хакеров
* DDos-атаки
* Таргетированные атаки
* Спам
* Фишинг
* Промышленные угрозы (stuxnet, flame, duqu)
* Шпионское программное обеспечение (spyware, adware)
* botnets (ботнеты или зомби-сети)