# Защита информации

# Концептуальные основы информационной безопасности

1. Законодательная и нормативная база правового регулирования вопросов защиты информации.
2. Исторические аспекты и современная постановка задач обеспечения информационной безопасности (ИБ) и защиты информации.
3. Связь проблем ИБ с развитием информационных технологий (ИТ) и процессами глобализации.
4. Основы российского законодательства в сфере защиты информации:
   1. закон об информации,
   2. информационных технологиях и защите информации;
   3. закон о государственной тайне;
   4. закон о защите персональных данных;
   5. закон об электронной цифровой подписи и т.д.
5. Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации.

## 1.1. Законодательная и нормативная база правового регулирования вопросов защиты информации

Информационная безопасность – это

защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения

<http://docs.cntd.ru/document/gost-r-50922-2006>

ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее  *конфиденциальность*, доступность и *целостность*.

* **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
* **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
* **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

**Угрозы информационной безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [[2](https://www.intuit.ru/studies/courses/697/553/literature#literature.2),[3](https://www.intuit.ru/studies/courses/697/553/literature#literature.3)]. **Атакой**называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

*Угроза* является следствием наличия уязвимых **мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

* по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
* по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
* по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
* по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:

1. законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
2. административный – комплекс мер, предпринимаемых локально руководством организации;
3. процедурный уровень – меры безопасности, реализуемые людьми;
4. *программно-технический уровень* – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

### ФЗ "Об информации, информационных технологиях и о защите информации"

URL: <http://www.consultant.ru/document/cons_doc_LAW_61798/>

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

* осуществлении права на поиск, получение, передачу,   
  производство и распространение информации;
* применении информационных технологий;
* обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

* **информация**- сведения (сообщения, данные) независимо от формы их представления;
* **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
* **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
* **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
* **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
* **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [[4](https://www.intuit.ru/studies/courses/697/553/literature#literature.4)].

В статье 4 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только федеральными законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;
7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся *информация* делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная *информация*, *доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *ограничение доступа* к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен федеральными законами.

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), если иное не предусмотрено федеральными законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

1. информацию, свободно распространяемую;
2. информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3. информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4. информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее *определение* защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа;
3. реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2. своевременное обнаружение фактов несанкционированного доступа к информации;
3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет  *права* и обязанности его субъектов.

Законодательство в области защиты информации:

1. Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».
2. № 1039101-6 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (№ 375-ФЗ от 6 июля 2016 г.)
3. № 1039149-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (№ 374-ФЗ от 6 июля 2016 г.)

<https://tass.ru/obschestvo/5914675>

В Госдуму внесли законопроект об автономной работе Рунета

В пояснительной записке отмечается, что документ подготовлен "с учетом агрессивного характера принятой в сентябре 2018 года стратегии национальной кибербезопасности США"

<https://meduza.io/news/2019/02/22/pravitelstvo-nachalo-sozdanie-tsentra-upravleniya-setyami-svyazi-senator-klishas-predlagal-ispolzovat-ego-dlya-izolyatsii-ot-interneta>

Премьер-министр Дмитрий Медведев подписал постановление о создании Центра мониторинга и управления сетью связи общего пользования. Роскомнадзор должен сделать это к 1 июля 2019 года.

4. Основы российского законодательства в сфере защиты информации:

* 1. закон об информации, информационных технологиях и защите информации http://www.consultant.ru/document/cons\_doc\_LAW\_61798/;
  2. закон о государственной тайне http://www.consultant.ru/document/cons\_doc\_LAW\_2481;
  3. закон о защите персональных данных https://rg.ru/2006/07/29/personaljnye-dannye-dok.html;
  4. закон об электронной цифровой подписи http://www.consultant.ru/document/cons\_doc\_LAW\_112701/.

## Практическая работа

1. Работа с зашифрованной почтой <http://protonmail.com/>

2.