## Создатель кибернетики Норберт Винер полагал, что информация обладает уникальными характеристиками и ее нельзя отнести ни к энергии, ни к материи. Особый статус информации как явления породил множество определений.

## В [словаре стандарта ISO/IEC 2382:2015](http://docs.cntd.ru/document/1200139532) «Информационные технологии» приводится такая трактовка:

## ***Информация (в области обработки информации)*** – любые данные, представленные в электронной форме, написанные на бумаге, высказанные на совещании или находящиеся на любом другом носителе, используемые финансовым учреждением для принятия решений, перемещения денежных средств, установления ставок, предоставления ссуд, обработки операций и т.п., включая компоненты программного обеспечения системы обработки.

Для разработки концепции обеспечения информационной безопасности (ИБ) под ***информацией*** понимают сведения, которые доступны для сбора, хранения, обработки (редактирования, преобразования), использования и передачи различными способами, в том числе в компьютерных сетях и других информационных системах.

Такие сведения обладают высокой ценностью и могут стать объектами посягательств со стороны третьих лиц. Стремление оградить информацию от угроз лежит в основе создания систем информационной безопасности.

## **Правовая основа**

В декабре 2016 года в России принята [новая редакция](https://searchinform.ru/blog/2016/12/07/osobye-zadachi-novoj-doktriny-informatsionnoj-bezopasnosti-rf/) Доктрины информационной безопасности. В документе ИБ определена как состояние защищенности национальных интересов в информационной сфере. Под национальными интересами в данном случае *понимается совокупность интересов общества, личности и государства, каждая группа интересов необходима для стабильного функционирования социума.*

Доктрина – концептуальный документ. Правоотношения, связанные с обеспечением информационной безопасности, регулируются федеральными законами «О государственной тайне», «Об информации», «О защите персональных данных» и другими. На базе основополагающих нормативных актов разрабатываются постановления правительства и ведомственные нормативные акты, посвященные частным вопросам защиты информации.

# **Особые задачи новой Доктрины информационной безопасности РФ**

Президент Российской Федерации Владимир Путин подписал указ об утверждении новой редакции Доктрины информационной безопасности. Указ вступает в силу с момента его подписания, при этом Доктрина от 2000 года признается утратившей силу.

Главными угрозами в новом документе признаны воздействие иностранных государств и «размывание духовно-нравственных ценностей». Как отмечают эксперты, изменения в Доктрине вызваны в основном политическими причинами – в частности, как ответная мера недавно принятой Европарламентом резолюции о противодействии «российской пропаганде».

«Доктрина информационной безопасности РФ была существенно переработана. Теперь она более конкретная, директивная и емкая. В документе выделяются три глобальные стратегические задачи:

1. Отдельно вынесена проблема недостаточного развития отрасли информационных технологий, сильная зависимость от иностранных продуктов и разработок. Доктрина призывает принять все необходимые меры, чтобы минимизировать влияние иностранных игроков.
2. В доктрине 2000 года упор делался на обеспечение свободного доступа любого гражданина к информационным ресурсам и технологиям связи. В новой редакции – на обеспечение безопасности взаимодействия людей с информационным пространством. Четко описывается стратегия обеспечения личной безопасности от технических угроз.
3. Следующий момент – стратегия обеспечения информационной безопасности РФ в глобальной сети. В новой доктрине сделан акцент на правдивом донесении информации о нашей стране, описан комплекс мер по соблюдению и достижению национальных интересов РФ в интернете, а также по обеспечению и защите конституционных прав граждан в цифровом пространстве. Заметно акцентировано внимание на противодействии «промывке мозгов» террористическими организациями и киберпреступлениям в кредитно-финансовой сфере.

В целом, документ отражает реалии и вопросы, стоящие перед Россией на ближайшее будущее».

**Определение информационной безопасности**

Прежде чем разрабатывать стратегию информационной безопасности, необходимо принять базовое определение самого понятия, которое позволит применять определенный набор способов и методов защиты.

Практики отрасли предлагают понимать под ***информационной безопасностью*** стабильное состояние защищенности информации, ее носителей и инфраструктуры, которая обеспечивает целостность и устойчивость процессов, связанных с информацией, к намеренным или непреднамеренным воздействиям естественного и искусственного характера. Воздействия классифицируются в виде угроз ИБ, которые могут нанести ущерб субъектам информационных отношений.

Таким образом, под ***защитой информации*** будет пониматься комплекс правовых, административных, организационных и технических мер, направленных на предотвращение реальных или предполагаемых ИБ-угроз, а также на устранение последствий инцидентов.

Непрерывность процесса защиты информации должна гарантировать борьбу с угрозами на всех этапах информационного цикла: в процессе сбора, хранения, обработки, использования и передачи информации.

Информационная безопасность в этом понимании становится одной из характеристик работоспособности системы. В каждый момент времени система должна обладать измеряемым уровнем защищенности, и обеспечение безопасности системы должно быть непрерывным процессом, которые осуществляется на всех временных отрезках в период жизни системы.

**Составляющие ИБ**



#### Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач являющимися равнозначными составляющими информационной безопасности.

#### **обеспечением доступности информации;**

#### **обеспечением целостности информации;**

#### **обеспечением конфиденциальности информации.**

**Доступность информации**

Роль доступности информации особенно проявляется в разного рода системах управления – производством, транспортом и т.п.

***Доступность информации*** — состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, хранение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов

**Доступность** – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. (получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно также получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило)

#### **Целостность информации**

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Целостность информации условно подразделяется на статическую и динамическую.

Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др. Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными и т.д. (рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным)

**Конфиденциальность**

Конфиденциальность – это защита от несанкционированного доступа к информации.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

## **Важность и сложность проблемы информационной безопасности**

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

Увеличение числа атак – ещё не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении и, как следствие, появляются новые виды атак.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведётся медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ – доступности, целостности или конфиденциальности.

Рассмотрим некоторую крупную организацию, например, оператора связи. Для неё характерно следующее:

- организация достаточно крупная и имеет территориально распределённую структуру, состоящую из нескольких филиалов;

- внутренний информационный обмен включает в себя одно или несколько крупных ключевых звеньев, требования к бесперебойности и корректности работы которых крайне высоки;

- имеется большой внешний информационный обмен с клиентами и партнерами;

- оператор связи, предоставляя своим заказчикам каналы связи, естественно, эти же каналы использует в собственной внутренней работе: в системах внутреннего документооборота, биллинговой системе и т.п.;

- значительное количество сотрудников, участвующих в информационном обмене, выезжают в командировки, где для них актуальна возможность продолжения полноценного информационного взаимодействия с ресурсами корпоративной информационной системы (КИС).