**Каждый день мы генерируем и обмениваемся огромными объемами данных, будь то личная переписка, финансовые транзакции или корпоративные секреты. Цифровая эпоха принесла не только удобство и новые возможности, но и**[**невиданные ранее вызовы**](https://beseller.by/blog/informatsionnaya-bezopasnost-i-kiberbezopasnost/#_ilyr5uopo64b)**, делая наши данные и системы потенциальной мишенью для различных угроз.**

Поэтому понимание того, [что такое информационная безопасность](https://beseller.by/blog/informatsionnaya-bezopasnost-i-kiberbezopasnost/#_khal11hs3kab), становится не техническим вопросом, а необходимостью для каждого, кто взаимодействует с цифровым пространством. Это очень широкая дисциплина, цель которой — защитить данные от несанкционированного доступа, искажения, уничтожения или нарушения ее доступности. Ответить на вопрос, как обеспечить эту защиту, означает осознать комплексность современных угроз и применить многоуровневый подход, охватывающий как технологии, так и ответственное поведение. Мы рассмотрим основные типы угроз, с которыми сталкиваются как компании, так и обычные пользователи, исследуем эффективные подходы и решения, позволяющие сохранить ценные данные в целости и сохранности.

Информационная безопасность (ИБ / Information Security) — это обширная сфера деятельности, которая занимается защитой [информации](https://beseller.by/#v3v2b9trfqxc) от несанкционированного доступа, использования, раскрытия, изменения, разрушения или нарушения ее работоспособности. Это не просто защита [данных](https://beseller.by/#38skqh3vl4r0) в цифровом виде, а системный подход к обеспечению сохранности всей информации, независимо от ее формы — будь то цифровая, бумажная или устная.

Основные принципы, на которых строится ИБ, часто обозначаются как «**триада КИД**»:

* **Конфиденциальность**. Этот принцип гарантирует, что доступ к информации имеют только авторизованные лица, что означает защиту от несанкционированного чтения или раскрытия данных. Например, банковские счета клиентов, медицинские записи или коммерческие тайны компании должны быть доступны строго определенному кругу лиц. Нарушение конфиденциальности может привести к утечке личных данных, шпионажу или недобросовестной конкуренции.
* **Целостность**. Принцип целостности обеспечивает точность и полноту информации, а также методов ее обработки. Это означает, что данные не были изменены или уничтожены несанкционированным образом, и что они остаются достоверными и надежными. Например, финансовые отчеты должны быть целостными, чтобы избежать ошибок или мошенничества. Нарушение целостности может привести к искажению данных, сбоям в системах или финансовым потерям.
* **Доступность**. Этот принцип гарантирует, что авторизованные пользователи могут получить доступ к информации и связанным с ней активам тогда, когда это им необходимо. Это означает, что системы, хранящие данные, и сетевая инфраструктура должны быть работоспособными и устойчивыми к сбоям. Например, веб-сайт электронной коммерции или система управления больницей должны быть доступны круглосуточно. Нарушение доступности может привести к простоям бизнеса, потере доходов или даже к угрозе жизни в критически важных системах.

Помимо этих трех столпов, информационная безопасность также включает в себя аспекты, связанные с **аутентификацией** (проверка личности пользователя), **авторизацией**(определение прав доступа пользователя), **неотказуемостью**(доказательство того, что действие было совершено определенной стороной) и **подотчетностью**(возможность отслеживать действия пользователей).

Инфобезопасность учитывает [**широкий спектр угроз**](https://beseller.by/blog/informatsionnaya-bezopasnost-i-kiberbezopasnost/#_tk3ujdf1o1kr), которые могут быть как **техническими**(например, вредоносное ПО), так и **организационными**(например, человеческая ошибка или несоблюдение политик), или даже **физическими**(например, кража ноутбука или пожар в серверной). [Она включает в себя](https://beseller.by/blog/informatsionnaya-bezopasnost-i-kiberbezopasnost/#_4bgnjrklhcl7) разработку политик, процедур, стандартов и руководств, а также внедрение соответствующих технологий и обучение персонала для минимизации рисков.

Кибербезопасность (Cybersecurity) — это одно из направлений в рамках обеспечения безопасность данных, которое сосредоточено на защите [информационных систем](https://beseller.by/#3bepztu2z7sl), сетей, программ, устройств и данных от цифровых атак, несанкционированного доступа, повреждения или уничтожения. Она действует в киберпространстве, где данные хранятся, обрабатываются и передается в электронном виде.

В фокусе кибербезопасности находятся методы, технологии и процессы, направленные на противодействие угрозам, возникающим именно в цифровой среде и включает в себя защиту от:

* **Вредоносного программного обеспечения**: вирусы, трояны, программы-вымогатели (шифровальщики), шпионское ПО, рекламное ПО, черви.
* **Фишинга и социальной инженерии**: попытки обманом заставить пользователей раскрыть конфиденциальную информацию или совершить нежелательные действия.
* **DDoS-атак**: атаки, направленные на вывод из строя сетевых ресурсов путем перегрузки их трафиком.
* **Уязвимостей в программном обеспечении и аппаратном обеспечении**: слабости, которые могут быть использованы злоумышленниками для получения несанкционированного доступа или нарушения работы систем.
* **Несанкционированного доступа к сетям и системам**: взломы, перехват сетевого трафика.

[Технические средства](https://beseller.by/blog/informatsionnaya-bezopasnost-i-kiberbezopasnost/#_p4s7wcgtco1e) кибербезопасности включают в себя использование антивирусного программного обеспечения, межсетевых экранов (файрволов), систем обнаружения и предотвращения вторжений (IDS/IPS), систем управления информацией и событиями безопасности (SIEM), шифрования данных, многофакторной аутентификации, а также проведение регулярных аудитов безопасности и тестирования на проникновение (пентестов). Кибербезопасность также включает в себя аспекты управления инцидентами, которые касаются реагирования на кибератаки и их последствий, а также восстановление после инцидентов.

**Кибербезопасность — «Цифровой меч и щит».**

Суть: Защита компьютерных систем, сетей и цифровых данных от кибератак.

* Цель: Бороться с угрозами из киберпространства (интернета, локальных сетей).
* Фокус: Технические аспекты:
	+ Взлом серверов, вирусы, фишинг, DDoS-атаки.
	+ Уязвимости в ПО, сетевом оборудовании, облачных сервисах.
* Методы:
	+ Межсетевые экраны (Firewall), антивирусы, системы обнаружения вторжений (IDS).
	+ Патчи безопасности, анализ вредоносного кода.

Пример: Отражение хакерской атаки на корпоративную сеть, восстановление данных после шифровальщика-вымогателя, настройка [VPN](https://beseller.by/#cf1hqcsc9uc7) для удаленных сотрудников.

**Основное различие между инфобезопасностью и кибербезопасностью заключается в их области охвата и фокусировке:**

Информационная безопасность — это всеобъемлющее понятие, которое охватывает защиту информации во всех ее формах, как цифровых, так и нецифровых, а также связанные с ней процессы и людей. Она ориентирована на обеспечение принципов конфиденциальности, целостности и доступности для всей информации организации или индивида.

Кибербезопасность является частью ИБ и сосредоточена конкретно на защите [информационных систем](https://beseller.by/#3bepztu2z7sl) и данных в цифровом пространстве. Она занимается угрозами, которые возникают исключительно из цифровой среды, и использует технические меры для их предотвращения и нейтрализации.

Если инфобезопасность заботится о том, чтобы важные документы не были украдены из сейфа (физическая безопасность), то кибербезопасность заботится о том, чтобы те же документы, если они хранятся на компьютере, не были украдены через интернет.

Информационная безопасность — стратегия защиты всех данных компании или человека любыми методами.

Кибербезопасность — тактический инструмент в рамках ИБ, сосредоточенный на отражении цифровых атак.

Без ИБ кибербезопасность слепа к нецифровым рискам. Без кибербезопасности ИБ беспомощна против хакеров.

Эти термины часто используются как взаимозаменяемые, особенно в неформальной речи, поскольку цифровая информация составляет подавляющее большинство данных, требующих защиты. Однако, для специалистов и в контексте построения комплексной системы защиты, важно понимать это различие для всестороннего и эффективного управления рисками.