

# Что такое информационная безопасность (InfoSec)?



---

Безопасность

---

26 июля 2024 года

---

✕ Закрыть

Здравствуйте! Как мы  
можем вам помочь?

## Авторы



**Джим Холдсворт**

Писатель



**Мэтью Косински**

Корпоративный  
технологический  
писатель

# Что такое информационная безопасность?

Информационная безопасность (InfoSec) - это защита важной информации от несанкционированного доступа, раскрытия, использования, изменения или нарушения. Это помогает обеспечить, чтобы конфиденциальные организационные данные были доступны авторизованным пользователям, оставались конфиденциальными и сохраняли свою целостность.

Нам необходимо защитить информационные активы, которые могут включать финансовые, конфиденциальные, личные или конфиденциальные данные. Эти активы могут принимать форму цифровых файлов и данных, бумажных документов, физических носителей и даже человеческой речи. На протяжении всего жизненного цикла данных InfoSec контролирует такие функции, как инфраструктура, программное обеспечение, тестирование, аудит и архивирование.

Основанная на многолетних принципах, информационная безопасность постоянно развивается для защиты все более гибридных и многообещающих сред в постоянно меняющемся ландшафте угроз. Учитывая развивающийся характер этих угроз, несколько команд работают над тем, чтобы обновить как технологии, так и процессы.

Цифровая информационная безопасность, [данных](#), сегодня получает наибольшее внимание от профессионалов в области информационной безопасности и находится в центре внимания этой статьи

Здравствуйте! Как мы можем вам помочь?

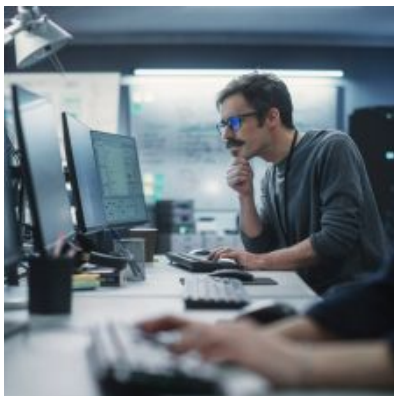
# Типы безопасности

Термины **информационной безопасности**, **ИТ-безопасности**, **кибербезопасности** и **безопасности данных** часто (и ошибочно) используются взаимозаменяемо. Хотя эти поля пересекаются и информируют друг друга, они различаются в первую очередь по сфере охвата.

- **Информационная безопасность** - это общий термин, который охватывает усилия организации по защите информации. Он включает в себя физическую безопасность ИТ-активов, безопасность конечных точек, [encryption](#) шифрование данных, [сетевую безопасность](#) и многое другое.
- **ИТ-безопасность** также связана с защитой физических и цифровых ИТ-активов и центров обработки данных, но не включает защиту для хранения бумажных файлов и других носителей. Он фокусируется на технологических активах, а не на самой информации.
- **Кибербезопасность** фокусируется на защите цифровых информационных систем. Цель состоит в том, чтобы помочь защитить цифровые данные и активы от киберугроз. Несмотря на огромное начинание, кибербезопасность имеет узкий охват, поскольку она не связана с защитой бумажных или аналоговых данных.
- **Безопасность данных** - это практика защиты цифровой информации от несанкционированного доступа, коррупции или кражи на протяжении всего жизненного цикла. Он включает в себя физическую безопасность оборудования и устройств хранения данных, а также административные средства и средства контроля доступа. Он также охватывает логическую безопасность программных приложений и организационных политик и процедур.

× Закрыть

Здравствуйте! Как мы можем вам помочь?



## Укрепляйте свою разведывательную базу безопасности

Будьте впереди угроз с новостями и идеями о безопасности, ИИ и многом другом, еженедельно в Think Newsletter.

Подписаться сегодня

# Почему InfoSec так важен

Данные питают большую часть мировой экономики, и киберпреступники признают ее ценность. [Кибератаки](#), направленные на кражу конфиденциальной информации — или, в случае [вымогателей](#), удержания данных в заложниках, стали более распространенными, разрушительными и дорогостоящими. Практика и принципы InfoSec могут помочь защитить данные перед лицом этих угроз.

Согласно [отчету](#) IBM средняя общая стоимость утечки данных достигла нового максимума в 4,45 миллиона долларов США в 2023 году. Эта цифра выросла на 15,3% с 3,86 млн долларов США в отчете за 2020 год.

Утечка данных обходится жертве несколькими способами. Неожиданный простоя приводит к потере бизнеса. Компания часто теряет клиентов и терпит значительный, а иногда и непоправимый ущерб своей репутации, когда конфиденциальная информация клиентов раскрывается. Украденная интеллектуальная собственность может повредить прибыльности компании и подорвать ее конкурентное преимущество.

Жертва утечки данных также может столкнуться с нормативными штрафами или юридическими штрафами. Правительство [Общий регламент по защите данных](#) (GDPR) и Закон о переносимости и подотчетности информации требуют, чтобы компании защищали конфиденциальную информацию своих клиентов. Невыполнение этого требования может привести к огромным штрафам.

✕ Закрыть

Здравствуйте! Как мы  
можем вам помочь?

Компании больше, чем когда-либо, инвестируют в технологии информационной безопасности и таланты. Согласно отчету о стоимости утечки данных, 51% организаций планируют увеличить инвестиции в безопасность после нарушения.

Основные области, выявленные для дополнительных инвестиций, включали планирование и тестирование реагирования на инциденты (ИК), обучение сотрудников и технологии обнаружения угроз и реагирования на них. Организации, которые сделали обширные инвестиции в ИИ и автоматизацию безопасности, сообщили о снижении затрат на утечку данных на 1,76 миллиона долларов по сравнению с организациями, которые не использовали возможности безопасности и возможности автоматизации.

Главные сотрудники по информационной безопасности (CISO), которые контролируют усилия по информационной безопасности, стали неотъемлемой частью корпоративных C-suites.

Спрос на аналитиков информационной безопасности, имеющих расширенные сертификаты информационной безопасности, такие как сертификация сертифицированных специалистов по безопасности информационных систем (CISSP) от ISC2. Бюро статистики труда прогнозирует занятость аналитиков информационной безопасности на 32% к 2032 году<sup>1</sup>

Смесь экспертов | 30 мая, эпизод 57

Присоединяйтесь к нашей группе инженеров мирового

класса, исследователей, лидеров продуктов и многого другого, поскольку они прорезают шум ИИ, чтобы принести вам последние новости и идеи ИИ.

[Смотреть последние эпизоды подкастов](#) →

## Принципы InfoSec

Методы информационной безопасности основаны на ряде многолетних, постоянно меняющихся принципов:

- **Триада ЦРУ**
- **Информационное обеспечение**
- **Неотчаяние**

## Триада ЦРУ

Впервые предложенная Национальным институтом стандартов и технологий (NIST) в 1977 году, триада ЦРУ предназначена для руководства организациями в выборе технологий, политики и практики для защиты своих информационных систем. Элементы триады ЦРУ включают:

- **Конфиденциальность**
- **Целостность**
- **Доступность**

**Конфиденциальность** означает, что стороны не могут получить доступ к данным, к которым они не имеют доступа.

Конфиденциальность определяет континуум пользователей, от привилегированных инсайдеров, имеющих доступ к большей части данных компании, до посторонних, уполномоченных просматривать только информацию, которую разрешено просматривать.

Личная информация должна оставаться конфиденциальной, а данные являются чувствительными. Если пароль к защищенным данным, это будет нарушением конфиденциальности.

Здравствуйте! Как мы можем вам помочь?

**Целостность** означает обеспечение того, чтобы вся информация, содержащаяся в базах данных компаний, была полной и точной.

Целостность направлена на то, чтобы остановить людей от фальсификации данных, таких как несанкционированные дополнения, изменения или удаления. Целостность данных применяется к предотвращению как противников, которые намеренно изменяют данные, так и пользователей с благими намерениями, которые изменяют данные несанкционированными способами.

**Доступность** означает обеспечение того, чтобы пользователи могли получить доступ к информации, к которой они имеют право получить доступ, когда они в ней нуждаются.


Доступность диктует, что меры и политика информационной безопасности не должны мешать авторизованному доступу к данным. Большая часть доступности проста, например, работа по обеспечению надежности аппаратного и программного обеспечения для предотвращения падения сайтов организации.

## Информационное обеспечение

Продолжающийся процесс достижения конфиденциальности, целостности и доступности данных в информационной системе известен как «информационная гарантия».

## Неотчаяние

Неотказ означает, что пользователь не может отрицать (то есть *отказать*) в совершении транзакции, например, изменении данных или отправке сообщения, потому что пользователю необходимо пройти [аутентификацию](#) для выполнения транзакции в первую очередь.

Хотя технически не является частью триады ЦРУ, неотказ от него с  [Заккрыть](#) аспекты конфиденциальности и целостности. Неотказ включает в себя обеспечение того, чтобы только авторизованные пользователи работали с данными, и чтобы они могли использовать только авторизованными способами.

Здравствуйте! Как мы можем вам помочь?

# Программы информационной безопасности

Специалисты по информационной безопасности применяют принципы InfoSec к информационным системам путем создания программ информационной безопасности. Эти программы представляют собой сборник политик информационной безопасности, мер защиты и планов, предназначенных для обеспечения информационной безопасности.


Основные компоненты программы информационной безопасности могут включать:

- **Оценка рисков**
- **Выявление уязвимостей**
- **Выявление угроз**
- **Планирование реагирования на инциденты**

## Оценка рисков

**Оценка рисков** информационной безопасности проверяет каждый аспект информационной системы компании. Оценка помогает специалистам по информационной безопасности понять точные риски, с которыми они сталкиваются, и выбрать наиболее подходящие **меры безопасности** и технологии для снижения рисков.

## Выявление уязвимостей

Уязвимость - это любая слабость в инфраструктуре информационных технологий (ИТ), которую противники могут использовать для получения несанкционированного доступа к данным. Например, хакеры могут воспользоваться ошибками в компьютерной программе, чтобы ввести вредоносное ПО или вредоносный код в законное приложение или  **Заккрыть**

Люди также могут создавать уязвимости в ИТ-системах. Например, киберпреступники могут манипулировать данными, если они делились конфиденциальной информацией инженерами, таких как фишинг.

Здравствуйте! Как мы можем вам помочь?



# Выявление угроз

Угроза - это все, что может поставить под угрозу конфиденциальность, целостность или доступность информационной системы.

Киберугроза — это угроза, которая использует цифровую уязвимость. Например, атака отказа в обслуживании (DoS) - это киберугроза, в которой киберпреступники подавляют часть информационной системы компании трафиком, вызывая ее сбой.

Угрозы также могут быть физическими. Стихийные бедствия, физические или вооруженные нападения и даже системные сбои оборудования считаются угрозами для информационной системы компании.

## Планирование реагирования на инциденты

[План реагирования на инциденты](#) (IRP) обычно направляет усилия организации по реагированию на инциденты.

Группы реагирования на инциденты с компьютерной безопасностью (CSIRT) часто создают и выполняют IRP с участием заинтересованных сторон из всей организации. Членами CSIRT могут быть главный сотрудник по информационной безопасности (CISO), [директор по ИИ \(CAIO\)](#), центр управления безопасностью (SOC), ИТ-персонал и представители юридических, [риск-менеджмента](#) и других нетехнологических дисциплин.

В ПИП подробно описаны шаги по смягчению последствий, которые организация предпринимает при обнаружении значительной угрозы. Хотя IRP варьируются в зависимости от организаций, которые их создают, и угроз, на которые они нацелены, общие шаги включают в себя:

- Соберите команду безопасности виртуально или лично.
- Проверьте источник угрозы.
- Действуйте, чтобы сдержать угрозу и с
- Определите, какой, если таковой имеется, был нанесен ущерб.

× Закрыть

Здравствуйте! Как мы можем вам помочь?

- Уведомлять заинтересованные стороны в организации, заинтересованные стороны и стратегических партнеров.

## ИнфоСек инструменты и методы

Программы информационной безопасности используют несколько различных инструментов и методов для устранения конкретных угроз. Общие инструменты и методы InfoSec включают в себя:

- **Криптография**
- **Предотвращение потери данных (DLP)**
- **Обнаружение и реагирование конечных точек (EDR)**
- **Брандмауэры**
- **Системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS)**
- **Системы управления информационной безопасностью (ISMS)**
- **Информация о безопасности и организация мероприятий (SIEM)**
- **Оперативные центры безопасности (SOC)**
- **Сильные меры по аутентификации**
- **Угрожающий интеллект**
- **Аналитика поведения пользователей и организаций (UEBA)**

## Криптография

**Криптография** использует алгоритмы для заслонения информации, так что только люди с разрешением и возможностью ее расшифровки могут прочитать.

## Предотвращение потери данных (DLP)

**DLP-стратегии** и инструменты отслеживают использование и перемещение данных по сети и обеспечивают соблюдение детальных политик безопасности, чтобы помочь предотвратить утечки и потери данных.

✕ Закрыть

## Обнаружение и реагирование конечных точек (EDR)

Здравствуй! Как мы можем вам помочь?

Решения [EDR](#) непрерывно отслеживают файлы и приложения на каждом устройстве, охотясь за подозрительной или вредоносной активностью, которая указывает на вредоносное ПО, вымогателей или расширенные угрозы.

## Брандмауэры

[Брандмауэр](#) - это программное или аппаратное обеспечение, которое останавливает подозрительный трафик от входа или выхода из сети, пропуская законный трафик. Брандмауэры могут быть развернуты на краях сети или использованы внутри, чтобы разделить большую сеть на более мелкие подсети. Если одна часть сети скомпрометирована, хакерам блокируют доступ к остальным.

## Системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS)

[IDS](#) - это инструмент сетевой безопасности, который отслеживает входящий сетевой трафик и устройства на предмет подозрительных нарушений политики безопасности или безопасности. [IPS](#) отслеживает сетевой трафик на предмет потенциальных угроз и автоматически блокирует их. Многие организации используют комбинированную систему, называемую **системой обнаружения и предотвращения вторжений (IDPS)**.

## Система управления информационной безопасностью (ISMS)

ISMS включает в себя руководящие принципы и процессы, которые помогают организациям защищать свои конфиденциальные данные и реагировать на нарушение данных. Наличие руководящих принципов также способствует преемственности, если есть большая текучесть кадров. [ISO/IEC 27001](#) является широко используемой ISMS.

## Информация о безопасности организация мероприятий

Здравствуйте! Как мы можем вам помочь?

Системы [SIEM](#) помогают обнаруживать аномалии поведения пользователей и использовать [искусственный интеллект \(ИИ\)](#) для автоматизации многих

ручных процессов, связанных с обнаружением угроз и реагированием на инциденты.

## Оперативный центр безопасности (SOC)

[SOC](#) объединяет и координирует все технологии и операции кибербезопасности под руководством команды специалистов по ИТ-безопасности, занимающихся круглосуточным мониторингом безопасности ИТ-инфраструктуры.

## Сильные меры по аутентификации

[Двухфакторная аутентификация \(2FA\)](#) и [многофакторная аутентификация \(MFA\)](#) являются методами проверки личности, в которых пользователи должны предоставить несколько доказательств, чтобы доказать свою личность и получить доступ к чувствительным ресурсам.

## Угрожающий интеллект

[Разведка угроз](#) помогает командам безопасности быть более активными, позволяя им предпринимать эффективные, основанные на данных действия для предотвращения кибератак до того, как они произойдут.

## Аналитика поведения пользователей и организаций (UEBA)

[UEBA](#) - это тип программного обеспечения безопасности, которое использует поведенческую аналитику и [алгоритмы машинного обучения](#) для выявления ненормального и потенциально опасного поведения пользователей и устройств.

## Угрозы информации безопасности

× Закрыть

Здравствуйте! Как мы можем вам помочь?

Организации сталкиваются с длинным списком потенциальных угроз информационной безопасности.

- Кибератаки
- Ошибка сотрудника
- Неэффективная безопасность конечных точек
- Инсайдерские угрозы
- Неправильная конфигурация
- Социальная инженерия

## Кибератаки

Эти атаки могут попытаться скомпрометировать данные организации с любого количества направлений, включая [расширенные атаки постоянных угроз \(APT\)](#), ботнеты (робот-сети), [распределенный отказ в обслуживании \(DDoS\)](#), атаки загрузки «привода» (которые автоматически загружают вредоносный код), [вредоносное ПО](#), [фишинг](#), вымогателей, вирусы и черви.

## Ошибка сотрудника

Люди могут потерять мобильное оборудование, загруженное конфиденциальной информацией, посетить опасные веб-сайты на оборудовании компании или использовать простые в трещинах пароли.

## Неэффективная безопасность конечных точек

Любой ноутбук, мобильное устройство или ПК может быть точкой входа в ИТ-систему организации при отсутствии адекватных антивирусных или [конечных решений безопасности](#).

## Инсайдерские угрозы

Существует два типа [инсайдерских угроз](#).

- Вредоносными инсайдерами являются авторизованные пользователи, которые используют информацию организации для личной выгоды
- Небрежные инсайдеры - это авторизованные пользователи, которые непреднамеренно ставят под угрозу безопасность, не следуя лучшим практикам

× Закрыть

Здравствуйте! Как мы можем вам помочь?

практикам безопасности.

Согласно отчету 32% инцидентов с безопасностью связаны со злонамеренным использованием законных инструментов. Инциденты включают кражу учетных данных, разведку, удаленный доступ и эксфильтрацию данных.

## Неправильная конфигурация

Организации полагаются на различные ИТ-платформы и инструменты, включая облачные возможности [хранения данных, инфраструктуру как услугу \(IaaS\)](#), интеграцию [программного обеспечения как услуги \(SaaS\)](#) и веб-приложения от различных поставщиков. Неправильные конфигурации любого из этих активов могут представлять риски безопасности.

Кроме того, поставщик или внутренние изменения могут привести к «дрифту конфигурации», где действительные настройки уходят в упадок.

*Индекс интеллекта угроз X-Force* сообщил, что во время тестирования [на проникновение](#) наиболее наблюдаемым риском веб-приложений в клиентских средах была неправильная конфигурация безопасности, составляющая 30% от общего числа.

## Социальная инженерия

Атаки [социальной инженерии](#) обманывают сотрудников, чтобы они разглашают конфиденциальную информацию или пароли, которые открывают дверь для злонамеренных действий.

Также может случиться так, что при попытке продвигать организацию через социальные сети сотрудники могут по ошибке разглашать слишком много личной или деловой информации, которая может быть использована злоумышленниками.

## Преимущества InfoSec

Преимущества сильной программы InfoSec организаций:

- Преемственность бизнеса

× Закрыть

Здравствуйте! Как мы можем вам помочь?