08 мая 2026

Информационная безопасность

Информационная безопасность бизнеса — это система организационных, технических и управленческих мер, направленных на защиту корпоративных данных, информационных систем и бизнес-процессов компании от утечек, взломов и внутренних ошибок.

Сегодня практически любой бизнес зависит от цифровой инфраструктуры. Финансовые операции, CRM-системы, базы клиентов, документы, аналитика и корпоративная коммуникация — всё это хранится в информационных системах. Потеря или компрометация этих данных может привести к финансовым потерям, штрафам и репутационным рискам.

Поэтому обеспечение информационной безопасности бизнеса перестало быть исключительно задачей IT-отдела. Это полноценная управленческая функция, которая влияет на устойчивость компании, её конкурентоспособность и стабильность бизнес-процессов.

Что такое информационная безопасность простыми словами

Если коротко, то информационная безопасность — это когда ваши данные в безопасности, а чужие глаза на них не смотрят. Хотя звучит это просто, за термином «информационная безопасность» (или просто ИБ) скрывается огромный пласт процессов, направленных на защиту практически всего, что

хранится в документах, файлах и базах. Представьте себе охранника, который следит не только за дверями, но и за тем, чтобы информация внутри не изменилась сама собой и была доступна именно тогда, когда она вам понадобилась.

Чаще всего понятия «информационная безопасность» и «кибербезопасность» путают, используя как синонимы. Но между ними есть принципиальная разница.

Кибербезопасность занимается защитой исключительно цифрового мира — ваших компьютеров, серверов и данных в интернете.

Информационная безопасность — понятие более ёмкое. Она переживает за всё: и за зашифрованные файлы, и за бумажный документ с печатью, лежащий в сейфе, и даже за переписку на салфетке, если эта переписка важна.

Весь этот цирк с паролями, шифрованием и бесконечными обновлениями держится на трёх простых принципах, которые специалисты с умным видом называют «Триадой CIA» (конфиденциальность, целостность, доступность).

- **Конфиденциальность.** Доступ к данным имеют только те, кому он действительно нужен, при этом секреты остаются секретами — ни больше ни меньше.
- **Целостность.** Данные должны оставаться в первозданном виде, без внезапных правок от левого пользователя. Нельзя, чтобы кто-то взял и

изменил сумму в договоре или удалил часть базы.

- **Доступность.** Информацией можно воспользоваться в любой момент. Бесполезно хранить данные под семью замками, если в критический момент до них невозможно добраться. DDoS-атаки как раз бьют по доступности, просто заваливая систему запросами.

Эти три столпа — база, на которой строится защита любого современного бизнеса, от маленького интернет-магазина до госкорпорации.

Почему ИБ — это не только про технику, но и про людей

Главная проблема всех систем безопасности, как ни странно, сидит перед экраном монитора и держит в руках кофе. Человеческий фактор остаётся самым слабым звеном в любой системе ИБ. Вы можете установить суперзащищённый файрвол, купить систему мониторинга за миллион, но один сотрудник, перешедший по ссылке из письма «Ваша посылка задержана» (фишинг), обнулит все усилия.

Именно поэтому современная информационная безопасность — это не просто набор софта и железа. Это культура, которую нужно прививать каждому, кто имеет доступ к данным. Сюда входят регулярные обучения, напоминания о правилах гигиены паролей и даже ворчливые письма от IT-отдела с требованием не хранить пароли на стикерах, приклеенных к монитору.

Здесь можно выделить несколько ключевых привычек:

- **Обновления всего и вся.** Операционные системы, программы и браузеры должны быть самыми свежими версиями. Разработчики закрывают уязвимости, о которых злоумышленники узнают первыми.
- **Сложные пароли.** Фраза «qwerty123» не подходит. Специалисты советуют использовать длинные пароли от 14 символов, непредсказуемые комбинации и генерировать уникальный ключ для каждого сервиса.
- **Двухфакторная аутентификация.** Даже если злоумышленник украдёт пароль, без кода из SMS или приложения-аутентификатора он не пройдёт. Это обязательный минимум для почты, соцсетей и тем более рабочих аккаунтов.

Зачем бизнесу информационная безопасность

Когда владельцы бизнеса слышат «информационная безопасность», они часто представляют бюджет под стать бюджету «Роскосмоса» или бесконечные запреты от IT-отдела. На практике обеспечение информационной безопасности бизнеса — это не про паранойю, а про устойчивость. Сколько вы потеряете, если база клиентов утечёт к конкуренту? Если производственная система встанет на три дня из-за шифровальщика? Если бухгалтер переведёт деньги по поддельному счёту «генерального директора»? Вот эти риски и есть то, чем занимается управление информационной безопасностью бизнеса. И это прямо влияет на прибыль.

Главное заблуждение: ИБ — это исключительно про хакеров и антивирусы. Нет. Для бизнеса это набор бизнес-процессов информационной безопасности, которые встроены в ежедневную рутину. От онбординга сотрудников (кому даём доступ к CRM) до офбординга (сразу отзываем

доступы при увольнении). От согласования договоров с новым подрядчиком до правил работы с ноутбуками в коворкинге. Если эти процессы не прописаны, то никакой «Тандер» вас не спасёт. Атаки на бизнес сегодня — это индустрия с готовыми скриптами, и они бьют не по коду, а по дырам в управлении.

Почему безопасность информационных систем бизнеса — это задача CEO, а не айтишника

Безопасность информационных систем бизнеса часто сводят к управлению паролями и установке фаерволов. И это логичная, но роковая ошибка.

Реальная защита начинается с ответа на вопрос: что для нас критично?

- Для интернет-магазина — это доступность сайта и база заказов.
- Для логистической компании — целостность данных о грузах.
- Для производственного предприятия — невозможность остановки станков через сеть.

Ответственность за определение «чему мы страхуемся в первую очередь» лежит не на системном администраторе, а на руководителе. Именно топ-менеджмент утверждает, сколько денег компания готова потерять в единицу простоя (RTO — целевое время восстановления) и какие данные нельзя потерять вообще. Затем эти цифры превращаются в задачи для организации информационной безопасности бизнеса: какие купить средства защиты, как часто делать бэкапы, кому разрешён удалённый доступ.

Типичная боль: когда ИБ мешает бизнесу. Например, требование менять сложный пароль каждые 14 дней приводит к тому, что сотрудники записывают их на стикеры. Гораздо эффективнее внедрить менеджеры паролей

(Bitwarden, Keeper) и двухфакторную аутентификацию через корпоративный SSO. Информационные технологии и безопасность бизнеса не должны конфликтовать — они должны быть спроектированы вместе. Там, где IT даёт инструмент, ИБ добавляет обёртку, которая не мешает работать.

Основные угрозы информационной безопасности бизнеса

Угрозы информационной безопасности бизнеса — это любые действия, события или уязвимости, которые могут привести к утечке данных, нарушению работы информационных систем или финансовым потерям компании. В корпоративной среде угрозы чаще всего направлены на критические информационные активы: базы клиентов, финансовые системы, корпоративную почту, CRM и ERP-платформы

Ниже приведены наиболее распространённые угрозы, с которыми сталкиваются компании.

Фишинг и социальная инженерия

Фишинг — это метод кибератаки, при котором злоумышленники пытаются обманом получить доступ к корпоративным данным. Обычно это происходит через поддельные письма, сайты или сообщения, которые выглядят как официальные уведомления от банков, партнёров или внутренних сервисов компании.

Сотрудник может перейти по вредоносной ссылке, ввести пароль от корпоративной почты или скачать заражённый файл. В результате злоумышленники получают доступ к внутренним системам, аккаунтам сотрудников и конфиденциальной информации.

Вредоносное программное обеспечение (Malware)

Вредоносное ПО — это программы, созданные для нарушения работы систем, кражи данных или получения несанкционированного доступа. К таким программам относятся вирусы, трояны, шпионское ПО и программы-шифровальщики (ransomware).

Например, ransomware может зашифровать все файлы на серверах компании и потребовать выкуп за восстановление доступа. Подобные атаки способны полностью остановить работу бизнеса на несколько дней или даже недель.

Утечки корпоративных данных

Утечка данных происходит, когда конфиденциальная информация выходит за пределы компании без разрешения. Это могут быть базы клиентов, коммерческие предложения, финансовые документы или стратегические планы развития.

Причины утечек бывают разными: ошибки сотрудников, неправильно настроенные системы доступа, использование незащищённых облачных сервисов или целенаправленные действия инсайдеров. Даже одна утечка клиентской базы может привести к серьёзным репутационным и финансовым последствиям.

Взлом корпоративных аккаунтов

Корпоративные аккаунты электронной почты, облачных сервисов и бизнес-приложений часто становятся целью атак. Если злоумышленник

получает доступ к учётной записи сотрудника, он может проникнуть во внутренние системы компании.

Причинами таких взломов обычно становятся слабые пароли, отсутствие многофакторной аутентификации или повторное использование паролей в разных сервисах. После взлома злоумышленники могут распространять вредоносные письма внутри компании или получать доступ к финансовым операциям.

DDoS-атаки на сервисы компании

DDoS-атака — это попытка вывести из строя сайт или онлайн-сервис компании путём массовой отправки запросов на сервер. В результате сервер не справляется с нагрузкой и перестаёт отвечать на реальные запросы пользователей.

Для интернет-магазинов, онлайн-сервисов и финансовых платформ такие атаки могут привести к прямым финансовым потерям и потере доверия клиентов.

Внутренние угрозы и человеческий фактор

Не все угрозы приходят извне. Иногда проблемы возникают внутри компании. Сотрудники могут случайно удалить важные данные, передать конфиденциальную информацию третьим лицам или использовать небезопасные устройства.

В некоторых случаях угрозу представляют бывшие сотрудники или недобросовестные работники, имеющие доступ к критически важной информации.

Если вы думаете, что вас не атакуют, потому что бизнес маленький, — вы ошибаетесь. Автоматизированные боты сканируют всю сеть и стучатся ко всем. Просто крупные компании получают целевые атаки, а малые — безликую рассылку троянов. И те, и другие горят одинаково.

Как построить организацию информационной безопасности бизнеса: три рабочих сценария

На практике организация информационной безопасности бизнеса зависит от размера компании. Вот три рабочих подхода.

Вариант А. Малый бизнес (до 50 человек)

Нет смысла нанимать штатного ИБ-специалиста. Используйте облачные сервисы со встроенной безопасностью (Яндекс 360 для бизнеса, Google Workspace, M365). Включите двухфакторную аутентификацию для всех, централизованное управление устройствами (MDM) и автоматические бэкапы всех критических данных в отдельное защищённое хранилище. Наймите внешнего ИБ-аудитора на полдня раз в квартал — он покажет типовые дыры.

Вариант Б. Средний бизнес (50–500 человек)

Уже нужен выделенный ответственный за ИБ (хотя бы на полставки) и прописанные бизнес-процессы информационной безопасности: процедура

инцидентов (кто что делает при утечке), политика парольной гигиены, план аварийного восстановления. Внедряйте SIEM-систему (например, MaxPatrol SIEM или Open Source аналог Wazuh) для сбора событий безопасности со всех серверов и рабочих станций. Обязательно — регулярное пентестирование (этичный взлом) силами внешней команды раз в полгода.

Вариант В. Крупный бизнес (500+)

Полноценный отдел информационной безопасности или аутсорсинг MSSP. Требуются формализованные процессы управления рисками (ISO 27001 или ГОСТ 57580.1-2017), система DLP для контроля утечек, отдельный план непрерывности бизнеса. Внедряйте классификацию данных: публичные, внутренние, конфиденциальные, секретные. Для каждой категории — свой уровень контроля и шифрования.

Отдельный совет: не гонитесь за сертификацией ISO 27001 с нуля, если не обязаны по договору с крупным заказчиком. Начните с самодиагностики по чек-листу. Самые болезненные места обычно лежат на поверхности: общие учётные записи, отсутствие бэкапов, незащищённый RDP-доступ к серверам.

Организация информационной безопасности бизнеса

Организация информационной безопасности бизнеса — это процесс построения комплексной системы защиты корпоративных данных,

IT-инфраструктуры и цифровых сервисов компании. Эта работа включает не только внедрение технологий, но и выстраивание управляемых процессов безопасности.

Обычно организация системы информационной безопасности проходит несколько этапов.

1. Инвентаризация информационных активов

На первом этапе компания определяет, какие данные и системы являются критически важными. Это могут быть CRM-системы, ERP-платформы, базы клиентов, финансовые сервисы, корпоративная почта и облачные хранилища.

Важно понять, где именно хранятся данные, кто имеет к ним доступ и как они используются в бизнес-процессах.

2. Анализ рисков и угроз

После определения активов проводится оценка рисков информационной безопасности. Специалисты анализируют потенциальные угрозы и уязвимости ИТ-инфраструктуры.

Например, проверяется защищённость сетей, конфигурация серверов, политика управления доступом и уровень защищённости пользовательских устройств.

3. Разработка политики информационной безопасности

На основе анализа рисков формируется политика информационной безопасности компании. Этот документ определяет правила работы с данными, порядок управления доступом, требования к паролям, правила использования корпоративных устройств и ответственность сотрудников.

Политика безопасности становится основой для построения всех процессов защиты информации.

4. Внедрение технических средств защиты

После разработки политики внедряются конкретные технические решения: системы защиты сети, мониторинг безопасности, средства контроля доступа и защиты данных.

Также на этом этапе внедряются системы резервного копирования, инструменты шифрования и средства обнаружения атак.

5. Обучение сотрудников и внедрение процессов

Даже самая современная система защиты не будет эффективной без подготовки сотрудников. Поэтому компании проводят регулярное обучение по вопросам информационной безопасности.

Сотрудников учат распознавать фишинговые письма, безопасно работать с данными и соблюдать корпоративные правила безопасности.

6. Мониторинг и аудит безопасности

Информационная безопасность — это непрерывный процесс. После внедрения системы защиты необходимо постоянно отслеживать события безопасности, проводить аудит ИБ и выявлять новые уязвимости.

Регулярные проверки помогают обнаружить слабые места до того, как ими воспользуются злоумышленники.

Обеспечение безопасности информационных систем бизнеса

Обеспечение безопасности информационных систем бизнеса строится на сочетании различных технологических решений. В корпоративной среде используется несколько ключевых классов систем защиты.

Системы управления доступом (IAM)

Identity and Access Management системы позволяют управлять доступом сотрудников к корпоративным ресурсам. Они контролируют, кто может входить в систему, какие данные просматривать и какие действия выполнять.

Примеры решений:

- Microsoft Entra ID (Azure AD)
- Okta
- Keycloak

Такие системы позволяют внедрять многофакторную аутентификацию и централизованно управлять правами пользователей.

SIEM-системы мониторинга безопасности

SIEM (Security Information and Event Management) собирают события из различных систем компании и анализируют их на предмет подозрительной активности.

Например, система может обнаружить массовые попытки входа в систему или необычную активность пользователя и автоматически уведомить службу безопасности.

Примеры SIEM-решений:

- IBM QRadar
- Splunk
- MaxPatrol SIEM

DLP-системы предотвращения утечек данных

DLP (Data Loss Prevention)предназначены для контроля передачи конфиденциальной информации за пределы компании. Такие системы анализируют электронную почту, файлы и сетевой трафик.

Если сотрудник пытается отправить клиентскую базу на личную почту или скопировать её на внешний носитель, система может автоматически заблокировать действие.

Примеры решений:

- SearchInform DLP
- InfoWatch Traffic Monitor
- Symantec DLP

Системы защиты конечных устройств (EDR/XDR)

EDR-решения защищают рабочие станции и серверы компании от вредоносного ПО и атак.

Они позволяют обнаруживать подозрительное поведение программ, блокировать вредоносные процессы и анализировать инциденты безопасности.

Примеры систем:

- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- Kaspersky EDR

Резервное копирование и восстановление данных

Даже при наличии сильной защиты полностью исключить инциденты невозможно. Поэтому важным элементом обеспечения безопасности является резервное копирование данных.

Системы backup позволяют быстро восстановить информацию после атак ransomware, аппаратных сбоев или ошибок сотрудников.

Примеры решений:

- Veeam Backup & Replication
- Acronis Cyber Protect
- Commvault

Почему бизнесу важен аудит информационной безопасности

Даже при наличии базовых средств защиты многие компании не имеют полного представления о реальном уровне безопасности своей ИТ-инфраструктуры. В системах могут оставаться уязвимости, которые годами остаются незамеченными.

Аудит информационной безопасности позволяет выявить слабые места инфраструктуры, оценить уровень защищённости данных и проверить соответствие требованиям законодательства и отраслевых стандартов.

Особенно актуален этот вопрос в условиях ужесточения требований к защите данных. Например, за утечку персональных данных компании могут получить крупные штрафы, а также столкнуться с судебными исками со стороны клиентов и партнёров. Кроме финансовых потерь, такие инциденты часто приводят к серьёзным репутационным рискам.

Компании, которые системно подходят к вопросам безопасности, регулярно проводят аудит инфраструктуры, тестирование на проникновение и оценку рисков.

В этом процессе бизнесу могут помочь специализированные консалтинговые компании. Например, КОРУС Консалтинг оказывает услуги по организации и развитию систем информационной безопасности бизнеса. Эксперты компании проводят аудит ИБ, анализируют риски, помогают внедрять системы защиты данных и выстраивать процессы управления безопасностью.

Такой подход позволяет не только снизить вероятность инцидентов, но и обеспечить соответствие требованиям законодательства и отраслевых стандартов безопасности.