# Security Engineering: часть 1. Введение и Человеческий фактор

Published: 09.06.2026 09:32 | Updated: 10.06.2026 11:35

# Инженерия безопасности: почему технологии бессильны без понимания людей

Информационная безопасность часто воспринимается исключительно как набор технических средств: шифрование, межсетевые экраны, антивирусы, системы обнаружения вторжений и средства контроля доступа. Однако такой взгляд отражает лишь небольшую часть реальной картины.
Мы рассмотрим гораздо более широкий подход. Он рассматривает безопасность как полноценную инженерную дисциплину, находящуюся на стыке технологий, экономики, психологии и организационного управления. Главная идея заключается в том, что безопасность нельзя свести к отдельным инструментам или продуктам. Это комплексный процесс проектирования систем, способных противостоять как случайным ошибкам, так и целенаправленным действиям злоумышленников.

## Что такое инженерия безопасности?

Безопасность отличается от обычной надежности систем одним важным фактором — наличием противника.
При проектировании надежных систем инженеры учитывают случайные сбои оборудования, программные ошибки и человеческие промахи. Однако в области безопасности необходимо учитывать существование злоумышленника, который активно ищет способы нарушить работу системы.
Определим инженерию безопасности следующим образом:

> «Инженерия безопасности занимается построением систем, которые остаются надежными перед лицом злоумышленника, ошибки или неудачи».

Эту идею хорошо иллюстрирует метафора Брюса Шнайера. Обычное программирование — это искусство заставить компьютер выполнять поставленные задачи. Надежное программирование предполагает учет случайных ошибок, возникающих из-за непредвиденных обстоятельств. Шнайер называет такой подход проектированием для «компьютера Мерфи».
Безопасное программирование требует совершенно иного мышления. Здесь приходится проектировать систему для условного «компьютера Сатаны» — противника, который будет целенаправленно искать любые уязвимости и использовать их в наиболее неблагоприятный момент.
Таким образом, безопасность — это не просто отсутствие ошибок. Это способность системы сохранять свои свойства даже в условиях активного противодействия.

# Фреймворк инженерии безопасности

Одной из важнейших концепций является модель, согласно которой безопасность опирается на четыре взаимосвязанных компонента. Ослабление любого из них способно поставить под угрозу всю систему.

## Политика безопасности (Policy)

Политика определяет цели безопасности и отвечает на вопрос:

> **Чего именно мы пытаемся достичь?**

Она формулирует правила, которым должна соответствовать система. Например:

- только врачи имеют доступ к историям болезни пациентов;
- сотрудник не может самостоятельно утверждать собственные финансовые операции;
- доступ к секретной информации предоставляется только лицам с соответствующим уровнем допуска.

Без четко сформулированной политики невозможно определить, что считать нарушением безопасности.

## Механизмы безопасности (Mechanism)

Механизмы представляют собой инструменты, используемые для реализации политики.
К ним относятся:

- криптографические алгоритмы;
- системы контроля доступа;
- биометрическая аутентификация;
- аппаратные средства защиты;
- физические замки;
- процедуры разделения обязанностей.

Важно понимать, что сами по себе механизмы не являются безопасностью. Они лишь обеспечивают выполнение заранее определенных правил.

## Гарантии безопасности (Assurance)

Наличие механизмов защиты не означает, что они действительно работают так, как задумано.
Гарантии отвечают на вопрос:

> **Насколько мы уверены, что механизмы корректно реализуют политику безопасности?**

Для получения такой уверенности используются:

- тестирование;
- аудит;
- независимая экспертиза;
- формальная верификация;
- сертификация;
- анализ архитектуры.

Без гарантий безопасность превращается из инженерной дисциплины в вопрос доверия и предположений.

## Стимулы участников системы (Incentives)

Многие проблемы безопасности возникают вовсе не из-за технических недостатков.
Зачастую причиной становятся неправильно выстроенные стимулы.

Необходимо понимать, почему пользователи, администраторы, организации и злоумышленники ведут себя именно так, а не иначе.
Ключевой вывод заключается в следующем:

> Системы часто ломаются не потому, что криптография слаба, а потому, что стимулы участников системы противоречат интересам безопасности.

Например, если банк перекладывает ответственность за мошеннические операции на клиента, у него исчезает экономический стимул инвестировать в совершенствование защитных механизмов. В результате уровень общей безопасности снижается.

# Почему стимулы имеют решающее значение

Тема стимулов становится одной из центральных идей безопасности.

## Проблема принципала и агента

Одной из ключевых экономических проблем является ситуация, когда лицо, принимающее решения, и лицо, несущее последствия этих решений, не совпадают.
Если организация не несет прямых убытков от недостаточного уровня безопасности, у нее может отсутствовать мотивация улучшать защиту.
Примером служат банкоматы. Если банк перекладывает ответственность за мошеннические операции на клиента, утверждая, что тот самостоятельно раскрыл PIN-код, стимулов инвестировать в повышение безопасности инфраструктуры становится значительно меньше.
Расходы несет клиент, а не организация.

## Рынок «лимонов» (Lemons Market)

Обратимся к концепции «рынка лимонов».
Проблема заключается в том, что потребители часто не способны оценить качество безопасности продукта до возникновения инцидента.
Если покупатель не может отличить действительно безопасное решение от небезопасного, он не готов платить больше за качество защиты.
Это создает стимул для производителей экономить на безопасности, выпуская дешевые, но уязвимые продукты. Постепенно рынок заполняется такими решениями.

### Безопасность как перенос риска

Иногда механизмы безопасности внедряются не столько для устранения угроз, сколько для перераспределения юридической ответственности между участниками процесса.
В подобных ситуациях безопасность превращается в инструмент управления рисками и ответственности, а не исключительно в средство защиты.

## Доверять или считать надежным: почему это не одно и то же

Одной из наиболее важных концепций понять различие между понятиями **trusted** и **trustworthy**. Несмотря на внешнюю схожесть, в инженерии безопасности они имеют принципиально разное значение.
Это различие часто игнорируется даже опытными специалистами, что приводит к ошибкам при проектировании защищенных систем.

### Trusted — доверенный компонент

**Trusted** — это компонент, отказ которого приведет к нарушению политики безопасности.
Другими словами, система вынуждена ему доверять независимо от того, заслуживает ли он этого доверия.
Например, операционная система пользовательского компьютера является доверенным компонентом. Если злоумышленник получит контроль над ней, безопасность всех остальных механизмов окажется под угрозой.
Важно понимать, что доверенный компонент не обязательно является надежным.
Яркий пример:

> Если сотрудник АНБ продает ключи китайскому дипломату, он остается trusted (доверенным), поскольку система была вынуждена ему доверять. Однако он явно не является trustworthy (заслуживающим доверия).

## Trustworthy — заслуживающий доверия компонент

**Trustworthy** обозначает компонент, который действительно обладает высоким уровнем надежности.
Такой компонент:

- тщательно протестирован;
- подвергся независимой проверке;
- спроектирован с учетом угроз;
- демонстрирует устойчивость к отказам и компрометации.

Именно к этому состоянию должны стремиться инженеры безопасности.

## Trusted Computing Base (TCB)

Различие между trusted и trustworthy приводит к еще одной фундаментальной концепции — **Trusted Computing Base (TCB)**.
TCB представляет собой совокупность всех компонентов системы, нарушение работы которых приведет к нарушению политики безопасности.
В состав TCB могут входить:

- аппаратное обеспечение;
- операционные системы;
- критически важное программное обеспечение;
- администраторы;
- процедуры управления;
- сотрудники организации.

Ключевая задача инженера безопасности заключается в следующем:

> Сделать TCB настолько небольшой, насколько это возможно.

Чем меньше доверенных компонентов присутствует в системе, тем проще:

- проводить аудит;
- анализировать угрозы;
- выполнять тестирование;
- обеспечивать высокий уровень надежности.

Идеальная цель состоит в том, чтобы максимально сократить количество **trusted-компонентов** и сделать их действительно **trustworthy**.

# Безопасность всегда зависит от контекста

Одной из центральных идей статьи является отказ от универсальных решений. Безопасность определяется не набором технологий, а контекстом, в котором функционирует система.
Одни и те же механизмы могут быть эффективны в одной сфере и совершенно непригодны в другой.
Для иллюстрации этой идеи рассмотрим четыре различных примера.

# Банк: когда главная угроза находится внутри

Интуитивно кажется, что банки должны защищаться прежде всего от внешних злоумышленников. Однако практика показывает обратное.

## Основная угроза

Существенная часть финансовых потерь связана с действиями собственных сотрудников.
Инсайдеры обладают:

- легитимным доступом к системам;
- пониманием внутренних процессов;
- знаниями о существующих механизмах контроля.

Поэтому именно внутренние угрозы становятся одним из главных рисков.

## Механизмы защиты

Для противодействия таким угрозам банки используют не только технические средства.
Ключевую роль играют организационные механизмы:

- **двойная бухгалтерия (Double-entry bookkeeping);**
- **разделение обязанностей (Separation of Duties);**
- процедуры аудита;
- взаимный контроль сотрудников.

Разделение обязанностей предполагает, что ни один сотрудник не должен иметь возможность самостоятельно выполнить критически важную операцию от начала до конца.

### Главный урок

В банковской сфере приоритетом часто становится **целостность (Integrity)** данных.
Деньги невозможно создать из ничего — их можно лишь перемещать между счетами.
Если сумма дебетовых операций не соответствует сумме кредитовых, система должна сигнализировать о наличии проблемы.
Этот пример показывает, что в некоторых областях целостность оказывается значительно важнее конфиденциальности.

## Военная база: защита информации любой ценой

Военные системы имеют совершенно иной профиль угроз.

### Основная угроза

Главную опасность представляют:

- внешние противники;
- шпионаж;
- утечки секретной информации.

Основной целью становится предотвращение несанкционированного распространения данных.

### Многоуровневая безопасность (MLS)

Для решения этой задачи используются модели **Multilevel Security (MLS)**.
Информация распределяется по уровням секретности:

- Несекретно;
- Для служебного пользования;
- Секретно;
- Совершенно секретно.

Основной принцип состоит в том, что информация должна перемещаться только в допустимых направлениях.
Упрощенно это можно описать как:

> Информация может двигаться вверх по уровням секретности, но не должна утекать вниз.

### Сложности модели

На практике подобные системы сталкиваются с рядом проблем.
Например:

- сложностью управления потоками информации;
- ошибками настройки политик доступа;
- существованием скрытых каналов передачи данных.

Особую опасность представляют вредоносные программы, способные проникать в высокозащищенные сегменты и передавать информацию менее защищенным системам.
Именно в этом контексте появляется модель **Bell–LaPadula**.

## Больница: когда безопасность конкурирует с доступностью

Медицинские учреждения сталкиваются с принципиально иной задачей.
Здесь безопасность представляет собой постоянный поиск компромисса.

### Конфликт интересов

Необходимо одновременно обеспечить:

- конфиденциальность медицинских данных пациентов;
- доступность информации для оказания своевременной медицинской помощи.

Чрезмерно строгие ограничения могут представлять прямую угрозу жизни пациента.

### Особенности медицинских систем

Военные системы работают по принципу:

> Нет допуска — нет доступа.

Однако в медицине подобный подход оказывается неприемлемым.
В экстренных ситуациях врач должен иметь возможность получить доступ к необходимой информации даже при отсутствии стандартных разрешений.

### Главный урок

Жесткие модели безопасности далеко не всегда подходят для реального мира. Многие системы требуют:

- учета контекста;
- гибкого принятия решений;
- баланса между безопасностью и функциональностью;
- учета этических аспектов.

Именно поэтому модели безопасности должны адаптироваться под особенности конкретной предметной области.

## Дом: размывание границ физической безопасности

Последний пример демонстрирует, как развитие технологий меняет само понимание безопасности.

### Эволюция угроз

Традиционно безопасность дома основывалась на физических механизмах:

- дверных замках;
- сигнализации;
- системах видеонаблюдения.

Однако появление устройств Интернета вещей радикально изменило ситуацию. Современный дом может содержать:

- умные замки;
- камеры наблюдения;
- голосовых помощников;
- интеллектуальные системы освещения;
- подключенные бытовые устройства.

### Новые риски

Раньше злоумышленнику требовалось физически проникнуть в помещение. Теперь атака может осуществляться удаленно.
Например, компрометация облачного сервиса производителя умного замка потенциально позволяет получить контроль над устройством без какого-либо физического контакта.

### Главный урок

Границы традиционного периметра безопасности постепенно исчезают. Сегодня физическая безопасность напрямую зависит от сетевой безопасности. Компрометация цифровых компонентов способна привести к вполне реальным последствиям в физическом мире.

## Основные выводы

Мы заложили фундаментальные принципы инженерии безопасности.

### Безопасность — это процесс, а не продукт

Невозможно просто приобрести «безопасность».
Необходимо постоянно:

- анализировать угрозы;
- пересматривать политики;
- совершенствовать механизмы защиты;
- проверять их эффективность;
- учитывать изменяющиеся стимулы участников системы.

### Человек является одновременно слабым звеном и частью решения

Игнорирование человеческого фактора неизбежно приводит к тому, что пользователи начинают обходить даже самые совершенные механизмы защиты. Психология и эргономика являются такими же важными компонентами безопасности, как криптография или контроль доступа.

### Контекст определяет требования к безопасности

То, что эффективно работает в банке, может оказаться бесполезным в больнице. То, что подходит для военных систем, способно сделать гражданские сервисы непригодными для использования.
Универсальных решений не существует.
Любая система безопасности представляет собой набор компромиссов между различными требованиями.
Эти выводы подготавливают нас к следующей важной теме: пониманию человеческой природы и её влияния на безопасность систем.

# Юзабилити и психология: почему люди становятся главной целью атак

До этого мы рассмотрели и теперь имеем представление что такое инженерия безопасности и как проектируются защищенные системы, то теперь сместим фокус внимания на человека.
Именно здесь одна из наиболее важных идей современной информационной безопасности:

> **Самым слабым звеном системы зачастую является не технология, а человек.**

Эта мысль хорошо отражена в известной цитате Брюса Шнайера:

> «Любители атакуют машины; профессионалы атакуют людей.»

Современные механизмы защиты становятся всё сложнее, криптографические алгоритмы совершенствуются, а вычислительные мощности растут. Однако злоумышленники все чаще предпочитают обходить технические барьеры и воздействовать непосредственно на пользователей.
Чтобы понять причины этого явления, необходимо обратиться к психологии человека.

## Почему человек становится слабым звеном

Компьютеры работают предсказуемо и детерминированно. Люди же действуют под влиянием эмоций, когнитивных ограничений, социальных норм и накопленного опыта.

Главная проблема заключается в том, что человеческий мозг эволюционировал для жизни в небольших социальных группах, а не для взаимодействия со сложными цифровыми системами.
Многие механизмы безопасности требуют от пользователей действий, к которым они попросту плохо приспособлены:

- запоминать десятки сложных паролей;
- оценивать подлинность сайтов;
- распознавать попытки социальной инженерии;
- принимать правильные решения под давлением времени.

Игнорирование этих ограничений делает даже технически совершенные системы уязвимыми.

## Асимметрия юзабилити

Обращаю внимание на важное различие между физическим и цифровым миром.
В физической среде многие предметы обладают естественной асимметрией использования.
Например, картофелечистка спроектирована таким образом, что очистить картофель значительно проще, чем причинить вред человеку.
Другими словами, правильное использование оказывается проще неправильного.
В цифровом мире ситуация часто оказывается противоположной.
Нажать на вредоносную ссылку значительно проще, чем проверить ее подлинность.
Передать пароль мошеннику может быть легче, чем правильно оценить уровень риска.
Таким образом, современные интерфейсы нередко создают среду, в которой ошибочные действия оказываются проще безопасных.

## Когнитивные ограничения человека

Человеческий мозг обладает ограниченными возможностями обработки информации.
Мы плохо справляемся с задачами, требующими:

- запоминания длинных случайных последовательностей символов;
- оценки вероятностей;
- постоянной концентрации внимания;

- обнаружения малозаметных аномалий.

При этом люди прекрасно распознают:

- лица;
- социальные сигналы;
- эмоциональные реакции;
- поведенческие шаблоны.

Системы безопасности, которые игнорируют эти особенности, неизбежно сталкиваются с сопротивлением пользователей и ростом числа ошибок.

# Социальная инженерия: эксплуатация человеческой природы

Социальная инженерия представляет собой использование психологических особенностей человека для получения несанкционированного доступа к информации или системам.
Вместо взлома технологий злоумышленник манипулирует людьми.
Выделяется два основных типа подобных атак.

# Претекстинг (Pretexting)

Претекстинг представляет собой создание убедительного сценария, который позволяет получить необходимую информацию.
Злоумышленник использует заранее подготовленную легенду и выдает себя за доверенное лицо.

## Как это работает

Атакующий может представляться:

- сотрудником технической поддержки;
- врачом;
- полицейским;
- коллегой;
- представителем банка;
- государственным служащим.

Основная цель состоит в том, чтобы вызвать доверие и убедить жертву добровольно предоставить необходимую информацию.

### Примеры

Примеры частных детективов, которые звонили в больницы или телекоммуникационные компании, выдавая себя за врачей или сотрудников полиции.
Используя авторитет и ощущение срочности, они получали доступ к конфиденциальным данным пациентов и абонентов.

### Практический эксперимент

Описывая эксперимент, в ходе которого сотрудников обучили проверять подозрительные телефонные запросы.
Несмотря на проведенное обучение, около тридцати ложных обращений еженедельно завершались успешно.
Этот результат демонстрирует, насколько сложно преодолеть естественную склонность человека доверять окружающим и стремление помочь собеседнику.

### Почему это работает

Претекстинг эксплуатирует фундаментальные особенности человеческого поведения:

- уважение к авторитету;
- стремление соблюдать социальные нормы;
- желание быть полезным;
- готовность реагировать на срочные ситуации.

Именно поэтому технические знания сами по себе не гарантируют устойчивость к подобным атакам.

## Фишинг (Phishing)

Фишинг представляет собой массовую рассылку поддельных сообщений, имитирующих коммуникацию от легитимных организаций.
Цель подобных атак заключается в получении:

- учетных данных;
- банковской информации;
- персональных данных;
- кодов подтверждения.

## Эволюция фишинга

Ранние фишинговые сообщения были достаточно примитивными и легко распознавались.
Типичным примером являются письма о наследстве от «нигерийских принцев».
Современные атаки стали значительно более изощренными.
Они используют:

- фирменный стиль известных компаний;
- правдоподобный дизайн;
- корректную терминологию;
- доменные имена, визуально похожие на настоящие;
- сценарии, вызывающие сильную эмоциональную реакцию.

Часто злоумышленники используют сообщения вроде:

> «Ваш аккаунт будет заблокирован.»

или

> «Подтвердите данные, чтобы избежать ограничения доступа.»

## Почему фишинг остается эффективным

Несмотря на высокий уровень осведомленности о подобных угрозах, фишинг продолжает успешно работать.
Причинами являются особенности человеческого восприятия.

### Поверхностная проверка URL

Большинство пользователей анализируют адрес сайта невнимательно.
Часто внимание концентрируется только на первых символах адреса или знакомом названии бренда.

### Доверие к визуальным признакам

Логотип компании, значок замка или привычный интерфейс формируют ощущение безопасности.
Пользователи склонны воспринимать такие элементы как доказательство подлинности ресурса.

**Эмоциональное воздействие**

Страх, жадность или ощущение срочности значительно снижают уровень критического мышления.
Именно поэтому злоумышленники активно используют эмоционально окрашенные сообщения.

# Ошибки и нарушения: важное различие

Важное разграничение между двумя типами небезопасного поведения пользователей.

## Ошибки (Slips and Mistakes)

Ошибки возникают в ситуациях, когда человек стремится выполнить правильное действие, но допускает промах.
Например:

- нажимает неправильную кнопку;
- случайно отправляет данные не тому получателю;
- забывает пароль;
- неверно интерпретирует сообщение системы.

Подобные проблемы обычно указывают на недостатки проектирования интерфейсов и процессов.

## Нарушения (Violations)

Нарушения возникают тогда, когда пользователь сознательно отказывается следовать установленным правилам.
Причинами могут быть:

- неудобство процедур;
- стремление ускорить работу;
- желание упростить выполнение задач;
- убежденность в избыточности ограничений.

Если сотрудник намеренно отключает защитные механизмы, поскольку они мешают работе, проблема заключается не только в пользователе, но и в неудачном проектировании системы безопасности.

# Когнитивные искажения: почему рациональные люди принимают небезопасные решения

Одной из ключевых идей является понимание того, что большинство ошибок пользователей обусловлено не недостатком интеллекта или знаний. Причина заключается в особенностях работы человеческого мышления.
Для быстрого принятия решений мозг использует так называемые **эвристики** — упрощенные правила, позволяющие экономить когнитивные ресурсы. В большинстве жизненных ситуаций они оказываются полезными, однако в сфере информационной безопасности нередко становятся источником уязвимостей.

## Эвристика доступности (Availability Heuristic)

Люди склонны оценивать вероятность событий на основе того, насколько легко соответствующие примеры приходят им в голову.
События, активно освещаемые в СМИ или недавно произошедшие в окружении человека, воспринимаются как более вероятные.

### Как это влияет на безопасность

Пользователи часто переоценивают редкие и зрелищные угрозы:

- атаки «суперхакеров»;
- сложные вирусы из фильмов;
- масштабные кибератаки на государства.

Одновременно они недооценивают значительно более распространенные риски:

- использование слабых паролей;
- повторное использование учетных данных;
- переход по фишинговым ссылкам;
- раскрытие информации в ходе социальной инженерии.

Например, человек может опасаться сложных технических атак, но без колебаний вводить пароль на поддельном сайте, поскольку подобная угроза кажется ему менее очевидной.

# Неприятие потерь (Loss Aversion)

Одним из фундаментальных открытий поведенческой экономики стало понимание того, что люди воспринимают потери значительно сильнее, чем аналогичные по величине приобретения.
Иными словами:

> Потеря 100 долларов вызывает более сильные эмоции, чем радость от получения тех же 100 долларов.

### Использование в атаках

Злоумышленники активно эксплуатируют этот психологический механизм. Фишинговые сообщения часто содержат предупреждения вроде:

- «Ваш счет будет заблокирован через 10 минут.»
- «Вы потеряете доступ к аккаунту.»
- «Для предотвращения списания средств срочно подтвердите личность.»

Страх потерять что-либо ценное заставляет людей действовать импульсивно и снижает способность к критическому анализу ситуации.

# Эффект привязки (Anchoring Effect)

Первичная информация оказывает непропорционально сильное влияние на дальнейшие оценки и решения.
После формирования первоначального впечатления человеку становится сложнее объективно анализировать последующие признаки.

### В контексте безопасности

Если письмо содержит:

- знакомый логотип банка;
- привычный дизайн;
- корректное обращение по имени;
- официальный стиль общения,

пользователь начинает воспринимать сообщение как легитимное.
Даже обнаружив подозрительные детали, такие как необычный URL или грамматические ошибки, он может проигнорировать их, поскольку первоначальное впечатление уже сформировано.

# Социальная психология и подчинение авторитету

Безопасность невозможно рассматривать вне социального контекста.
Человеческое поведение во многом определяется окружающими людьми и общественными нормами.
Обратимся к классическим психологическим экспериментам, демонстрирующим, насколько сильно социальное влияние определяет наши действия.

# Эксперимент Милгрэма: подчинение авторитету

Психолог Стэнли Милгрэм исследовал готовность людей подчиняться указаниям авторитетной фигуры.
Участникам эксперимента предлагалось наносить другим людям удары электрическим током возрастающей силы за ошибки при выполнении заданий.
Несмотря на очевидный дискомфорт и моральные сомнения, значительная часть испытуемых продолжала выполнять указания экспериментатора.

## Значение для информационной безопасности

Люди склонны выполнять требования тех, кого считают представителями власти или авторитетными специалистами.
Именно поэтому злоумышленники часто представляются:

- сотрудниками технической поддержки;
- представителями правоохранительных органов;
- системными администраторами;
- сотрудниками банка;
- руководителями организации.

Если человек воспринимает собеседника как авторитет, вероятность выполнения опасных инструкций существенно возрастает.
Пользователь может:

- сообщить пароль;
- установить вредоносное программное обеспечение;
- предоставить доступ к системе;
- раскрыть конфиденциальную информацию.

При этом он может искренне считать свои действия правильными.

# Эксперимент Аша: сила конформизма

Соломон Аш исследовал влияние группового мнения на принятие решений.
В ходе эксперимента участникам демонстрировали очевидно неправильные ответы группы на простые визуальные задачи.
Несмотря на очевидность ошибки, многие испытуемые соглашались с большинством.

### Значение для безопасности

Поведение окружающих оказывает существенное влияние на соблюдение правил безопасности.
Если внутри организации сотрудники:

- используют простые пароли;
- игнорируют предупреждения браузеров;
- обходят защитные механизмы;
- не соблюдают установленные процедуры,

новые сотрудники с высокой вероятностью перенимают аналогичное поведение.
Культура безопасности внутри организации может быть не менее важной, чем используемые технические средства защиты.

# Когнитивный диссонанс

Люди стремятся поддерживать внутреннюю согласованность своих убеждений и поступков.
Осознание того, что человек стал жертвой мошенничества, вызывает психологический дискомфорт.
Для снижения этого дискомфорта возникает тенденция рационализировать собственные действия.

### Как это используют злоумышленники

После совершения первого небольшого действия человек становится более склонным к дальнейшему участию.
Например:

1. Пользователь переходит по ссылке из подозрительного письма.
2. Затем вводит имя пользователя.
3. После этого предоставляет пароль.

4. Позже подтверждает операцию кодом из SMS.

На каждом этапе человеку становится психологически сложнее признать, что он совершает ошибку.
Вместо этого он стремится оправдать свои предыдущие решения, продолжая взаимодействие с мошенниками.

## Почему обучение пользователей не всегда эффективно

Традиционный подход к безопасности предполагает, что достаточно обучить пользователей правильному поведению.
Однако относится к подобному взгляду можно достаточно скептически.
Причины очевидны:

- когнитивные ограничения невозможно полностью устранить;
- эмоциональное давление влияет даже на подготовленных специалистов;
- социальные механизмы действуют независимо от уровня технических знаний;
- постоянная бдительность требует значительных психологических ресурсов.

Даже хорошо информированные пользователи могут становиться жертвами социальной инженерии.
Это означает, что безопасность не должна полностью перекладываться на человека.

## Проектирование систем с учетом человеческой природы

Поскольку человеческие ошибки неизбежны, системы безопасности должны проектироваться таким образом, чтобы минимизировать последствия этих ошибок.
Основные принципы такого подхода включают:

- снижение когнитивной нагрузки;
- предотвращение ошибок по умолчанию;
- использование безопасных настроек по умолчанию;
- создание понятных интерфейсов;
- внедрение дополнительных уровней защиты.

Инженер безопасности должен исходить не из предположения, что пользователи будут действовать идеально, а из понимания того, что:

> Люди будут ошибаться, отвлекаться, торопиться и иногда принимать неверные решения.

Именно поэтому задача проектировщика заключается не в изменении человеческой природы, а в создании систем, устойчивых к ее проявлениям.

## Пароли: компромисс между безопасностью и человеческими возможностями

Несмотря на появление новых методов аутентификации, пароли остаются одним из наиболее распространенных механизмов защиты цифровых систем.
Однако именно они представляют собой одну из самых проблемных областей информационной безопасности.
Главная причина заключается в том, что парольные системы требуют от людей выполнения задач, к которым человеческая память плохо приспособлена.
Пользователям необходимо:

- создавать сложные секреты;
- запоминать десятки уникальных комбинаций;
- регулярно обновлять их;
- не записывать;
- не использовать повторно;
- распознавать попытки их компрометации.

На практике подобные требования часто оказываются нереалистичными.

## Почему пароли становятся проблемой

Человеческая память хорошо работает с информацией, обладающей смыслом и ассоциативными связями.
Случайные последовательности символов, напротив, запоминаются крайне плохо.
Поэтому пользователи естественным образом стремятся упростить задачу.
Это приводит к появлению предсказуемых моделей поведения.

# Типичные ошибки пользователей

## Использование простых паролей

Многие пользователи выбирают пароли, основанные на легко запоминаемой информации:

- именах;
- датах рождения;
- именах домашних животных;
- общеупотребительных словах;
- последовательностях символов (123456, `qwerty`).

Подобные комбинации легко поддаются словарным атакам.

## Повторное использование паролей

Одной из наиболее распространенных практик является использование одного и того же пароля на множестве различных сервисов.
Причины такого поведения очевидны:

- ограниченные возможности памяти;
- стремление снизить когнитивную нагрузку;
- удобство использования.

Однако компрометация одного сервиса автоматически ставит под угрозу все остальные учетные записи пользователя.
Даже если крупные платформы обладают хорошей защитой, утечка данных из менее защищенного сайта может привести к компрометации критически важных аккаунтов.

## Запись паролей

Традиционно организации запрещают пользователям записывать пароли.
Однако стоит обратить внимание на интересный парадокс.
Записанный и надежно хранящийся пароль иногда оказывается безопаснее, чем один простой пароль, используемый на десятках различных сервисов.
Например, сложный уникальный пароль, записанный и хранящийся в сейфе, может представлять меньший риск, чем легко угадываемый пароль,

применяемый повсеместно.
Это наблюдение подчеркивает важность учета реального поведения пользователей при разработке политик безопасности.

# Проблема секретных вопросов

Многие системы используют контрольные вопросы для восстановления доступа. Типичными примерами являются вопросы:

- девичья фамилия матери;
- имя первого домашнего животного;
- школа, которую посещал пользователь;
- место рождения.

Подобный подход имеет фундаментальные недостатки.

## Информация не является секретной

В современном мире значительная часть подобных сведений может быть получена через:

- социальные сети;
- открытые государственные реестры;
- утечки персональных данных;
- общедоступные базы информации.

## Секрет невозможно изменить

Если пароль был скомпрометирован, его можно заменить.
Однако невозможно изменить:

- биографические факты;
- семейные связи;
- события прошлого.

После компрометации подобных данных восстановление безопасности становится значительно сложнее.
Рассматриваем использование таких вопросов как крайне ненадежный механизм аутентификации.

# Принудительная смена паролей: благие намерения и реальные последствия

На протяжении многих лет распространенной практикой являлось требование регулярно менять пароли.
Часто организации устанавливали обязательную смену каждые:

- 30 дней;
- 60 дней;
- 90 дней.

Предполагалось, что подобная мера ограничит время использования украденных учетных данных.
Однако на практике результаты оказались далеко не однозначными.

## Как ведут себя пользователи

Большинство людей не создают полностью новые сложные пароли.
Вместо этого они используют небольшие вариации уже существующих комбинаций:

- `Password01`
- `Password02`
- `Password03`

или

- `Summer2025`
- `Summer2026`

Подобные шаблоны легко предсказываются злоумышленниками.

## Непредвиденные последствия

Частая смена паролей приводит к росту числа небезопасных практик:

- записи паролей на бумаге;
- хранения их в незашифрованных файлах;
- использования предсказуемых последовательностей;
- увеличения нагрузки на службы поддержки.

Таким образом, политика, направленная на повышение безопасности, способна приводить к обратному эффекту.
Этот пример хорошо демонстрирует важность учета человеческого поведения при разработке защитных механизмов.

# Атаки на процесс ввода паролей

Даже если пользователь создал надежный пароль, он может быть скомпрометирован в момент ввода.

# Подглядывание через плечо (Shoulder Surfing)

Одним из простейших методов является непосредственное наблюдение за пользователем.
Злоумышленник может получить пароль, наблюдая за вводом:

- в общественных местах;
- в офисах;
- возле банкоматов;
- в транспорте.

Особенно уязвимыми оказываются короткие PIN-коды.
Подобные атаки не требуют сложных технических средств и полностью обходят криптографическую защиту.

# Кейлоггеры (Keyloggers)

Кейлоггеры предназначены для регистрации нажатий клавиш пользователя.
Они могут существовать в различных формах.

## Программные кейлоггеры

Представляют собой вредоносное программное обеспечение, устанавливаемое на устройство жертвы.
После установки они способны фиксировать:

- логины;
- пароли;
- номера банковских карт;
- содержимое переписки.

### Аппаратные кейлоггеры

Являются физическими устройствами, подключаемыми между клавиатурой и компьютером.
Такие устройства могут длительное время оставаться незамеченными и собирать вводимую информацию.

## Экранные клавиатуры и их ограничения

Для борьбы с кейлоггерами некоторые финансовые организации внедряли виртуальные клавиатуры.
Пользователь вводил пароль при помощи мыши, нажимая кнопки на экране.
Предполагалось, что отсутствие нажатий физических клавиш предотвратит перехват информации.
Однако злоумышленники быстро адаптировались.
Современные вредоносные программы способны:

- делать снимки экрана;
- отслеживать координаты курсора;
- анализировать последовательность кликов мышью.

Таким образом, виртуальные клавиатуры не устранили проблему полностью.

## Атаки на хранение паролей

Даже идеально организованный процесс ввода не защищает пользователей, если компрометируется система хранения учетных данных.

## Хеширование паролей

Вместо хранения паролей в открытом виде системы обычно сохраняют их криптографические хеши.
При вводе пароля:

1. система вычисляет его хеш;
2. сравнивает результат с сохраненным значением;
3. предоставляет доступ только при совпадении.

Это позволяет избежать хранения исходных паролей.
Однако подобный подход не гарантирует абсолютную безопасность.

## Словарные атаки

Злоумышленник может последовательно вычислять хеши распространенных паролей и сравнивать их с украденной базой данных.
Если пользователи выбирают слабые комбинации, компрометация происходит достаточно быстро.

## Радужные таблицы (Rainbow Tables)

Радужные таблицы представляют собой заранее вычисленные наборы соответствий между паролями и их хешами.
Использование таких таблиц позволяет значительно ускорить подбор учетных данных.
Если система хранит хеши без дополнительных механизмов защиты, атака становится существенно проще.

## Значение соли (Salt)

Для противодействия подобным атакам используются случайные значения — **соль (salt)**.
Соль добавляется к паролю перед вычислением хеша.
В результате одинаковые пароли разных пользователей приводят к различным хешам.
Это делает применение заранее подготовленных радужных таблиц значительно менее эффективным.

## Пример уязвимости WordPress

Приведем пример архитектурного решения, демонстрирующего, насколько опасными могут быть ошибки при проектировании систем аутентификации.
В одной из реализаций WordPress в cookie-файлах хранились значения, производные от хеша пароля.
Если злоумышленник получал доступ к базе данных с учетными записями, он мог использовать имеющуюся информацию для входа в систему администратора, не зная исходного пароля.
Этот пример показывает важную закономерность:

> Безопасность системы определяется не только надежностью криптографических алгоритмов, но и корректностью их применения.

Даже использование сильных криптографических примитивов не защищает от ошибок проектирования.

# Главный урок парольной аутентификации

Большинство проблем, связанных с паролями, возникает не из-за недостатков пользователей или слабости алгоритмов.
Основная причина заключается в несоответствии между возможностями человека и требованиями, предъявляемыми системой безопасности.
Если защитный механизм требует от людей невозможного, пользователи неизбежно начинают искать обходные пути.
Поэтому эффективные системы аутентификации должны учитывать реальные особенности человеческого поведения, а не предполагать существование идеальных пользователей.

# Двухфакторная аутентификация (2FA)

Одним из наиболее распространенных способов повышения безопасности учетных записей является использование двухфакторной аутентификации.

Ее идея заключается в комбинировании нескольких независимых факторов:

- **то, что вы знаете** (пароль);
- **то, что у вас есть** (телефон, токен, устройство);
- иногда также **то, чем вы являетесь** (биометрия).

## Как это работает

Даже если злоумышленник получает пароль пользователя, он не может войти в систему без второго фактора подтверждения.
Это значительно усложняет процесс атаки, особенно при массовом фишинге или утечках баз данных.

## Ограничения 2FA

Несмотря на эффективность, двухфакторная аутентификация не является абсолютной защитой.
Важное ограничение — **атаки типа “man-in-the-middle” в реальном времени**.

### Атака «человек посередине»

В таких сценариях злоумышленник действует следующим образом:

1. Пользователь вводит данные на поддельном сайте.
2. Сайт в реальном времени передает эти данные на настоящий сервис.
3. Система отправляет код подтверждения пользователю.
4. Пользователь вводит код.
5. Злоумышленник мгновенно использует его для входа в систему.

Таким образом, даже одноразовые коды могут быть перехвачены и использованы в режиме реального времени.

## Биометрическая аутентификация: удобство и иллюзия безопасности

Биометрические методы (отпечатки пальцев, распознавание лица, радужная оболочка глаза) активно используются как средство повышения удобства.

### Преимущества

- не требуется запоминать пароль;
- быстрое подтверждение личности;
- удобство использования в повседневных сценариях.

### Фундаментальная проблема

Биометрические данные не являются секретом в классическом смысле.
В отличие от пароля:

- отпечатки пальцев остаются на предметах;
- лицо можно сфотографировать;
- голос можно записать.

### Невозможность замены

Если биометрические данные скомпрометированы, их невозможно «сменить».
Нельзя заменить:

- отпечатки пальцев;
- структуру лица;
- радужную оболочку глаза.

Это делает биометрию уязвимой как единственный фактор аутентификации.

### Вывод

Биометрия может использоваться как дополнительный фактор, но не как единственный механизм защиты.

## CAPTCHA: защита от автоматизации

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) используется для различения людей и автоматических программ.

### Основная идея

Пользователь должен выполнить задачу, которую легко решить человеку, но сложно автоматизировать:

- распознавание искаженного текста;
- выбор изображений;
- логические задачи.

### Проблемы CAPTCHA

Несмотря на полезность, этот механизм имеет ряд ограничений:

- ухудшает пользовательский опыт;
- создает барьеры для людей с ограниченными возможностями;
- постепенно становится уязвимым к современным алгоритмам машинного обучения;
- может быть обходится через «фермы CAPTCHA», где задачи решаются реальными людьми за оплату.

Таким образом, CAPTCHA не является абсолютным решением проблемы автоматизированных атак.

## Почему обучение пользователей недостаточно

Одним из распространенных подходов к безопасности является обучение пользователей правильному поведению.
Однако подчеркивается, что этот подход имеет фундаментальные ограничения.

### Причины неэффективности обучения

- когнитивные ограничения человека невозможно устранить обучением;
- эмоциональное давление снижает критическое мышление;
- социальная инженерия действует независимо от уровня знаний;
- постоянная бдительность требует значительных психических ресурсов.

Даже хорошо подготовленные специалисты могут становиться жертвами атак.

### Вывод

Нельзя полагаться только на обучение пользователей как на основной механизм защиты.

## Системный подход к безопасности

Основной вывод статьи заключается в необходимости проектировать системы с учетом реального поведения людей.

### Принципы проектирования

#### 1. Снижение когнитивной нагрузки

Система должна минимизировать требования к памяти и вниманию пользователя:

- использование менеджеров паролей;
- автоматизация аутентификации;
- упрощение интерфейсов.

#### 2. Безопасность по умолчанию

Система должна быть защищенной даже при неправильных действиях пользователя.
Ошибки не должны приводить к критическим последствиям.

#### 3. Предотвращение ошибок

Интерфейсы должны проектироваться так, чтобы уменьшать вероятность случайных действий:

- подтверждения критических операций;

- понятные предупреждения;
- ограничения опасных действий.

**4. Реалистичное моделирование пользователя**

Инженер должен исходить из того, что:

- пользователи ошибаются;
- пользователи спешат;
- пользователи отвлекаются;
- пользователи могут быть обмануты.

# Главный итог

Подводим к фундаментальному выводу:

> Безопасность системы определяется не только криптографией и техническими механизмами, но и поведением человека, который с этой системой взаимодействует.

Игнорирование человеческого фактора приводит к тому, что даже самые сложные защитные механизмы оказываются уязвимыми.
Поэтому инженерия безопасности должна учитывать психологию, поведение и реальные ограничения пользователей наравне с техническими аспектами системы.