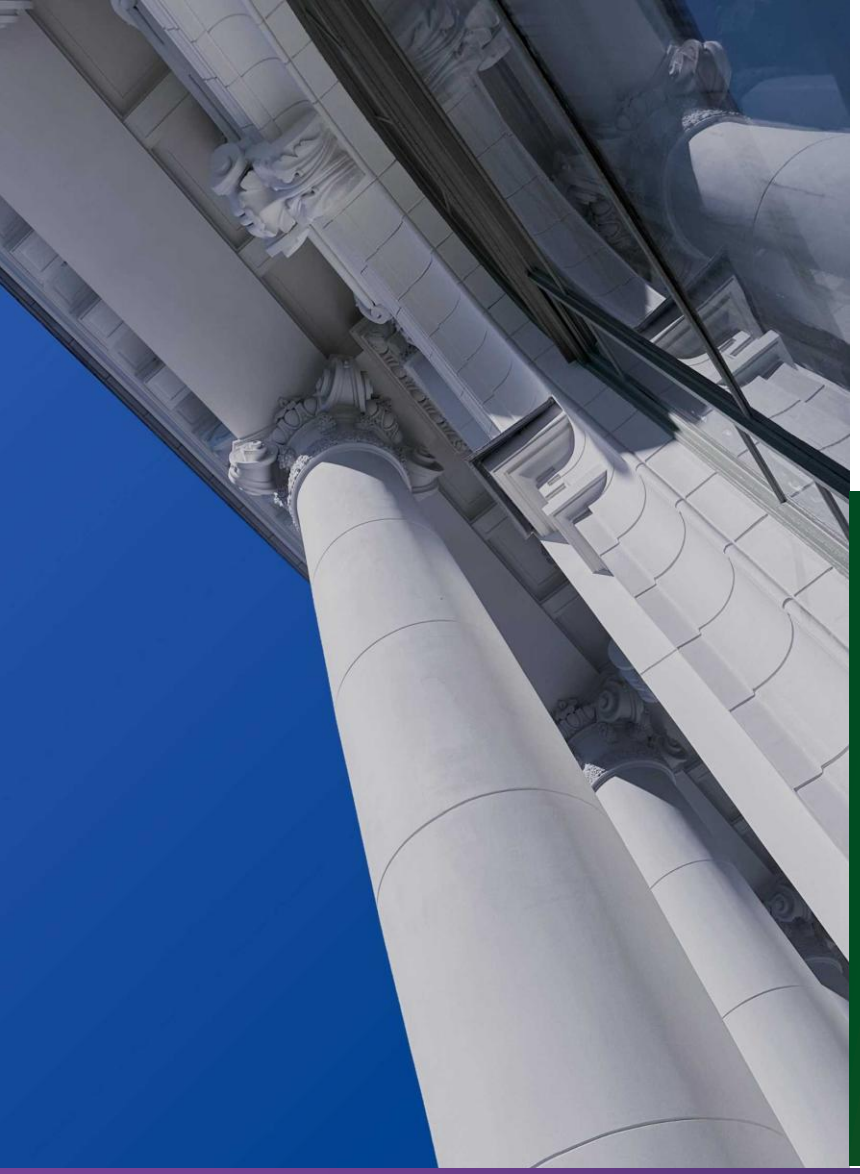


Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

Высшая школа биомедицинских систем и технологий

ПОЛИТЕХ

2025

Угрозы информационной безопасности

Выполнили: студенты группы №4731204/50001
Горохова Ангелина
Дурнева Вероника
Перькова Кира
Преподаватель: Горелов Сергей Васильевич

Введение

ПОЛИТЕХ

Проблема:

Неспособность традиционных систем безопасности эффективно противостоять современным, эволюционирующим и комплексным киберугрозам.

Актуальность:

Прямое влияние на национальную и экономическую безопасность. Атаки на критическую информационную инфраструктуру (КИИ) — энергетику, финансы, транспорт — могут парализовать жизнь целых регионов. В связи с этим государства, включая Россию (через такие законы, как 187-ФЗ), ужесточают регулирование, переводя вопросы кибербезопасности из разряда технических в разряд стратегических.

Информационная безопасность — это совокупность мер по защите данных от несанкционированного доступа, изменений, уничтожения или потери. Защита обеспечивается с помощью специальных инструментов и подходов.

Угрозы информационной безопасности — это действия или события, которые могут нанести ущерб информационным системам, привести к утечке, потере или повреждению данных.

Рис.1 Информацинная безопасность

Классификация угроз

По месту возникновения

- Внешние
- Внутренние

По объективности

- Случайные
- Преднамеренные

По видимости

- Явные
- Неявные

По доступу

- Неавторизованный доступ
- Авторизованный доступ

По цели

- Угрозы на разрушение
- Угрозы на кражу данных
- Угрозы на шантаж

По способу реализации

- Технические
- Социальные
- Физические

Основные виды информационных угроз

ПОЛИТЕХ

- Вредоносное ПО
- Фишинг
- Внутренние угрозы
- Угрозы в облачных сервисах
- DDoS-атаки

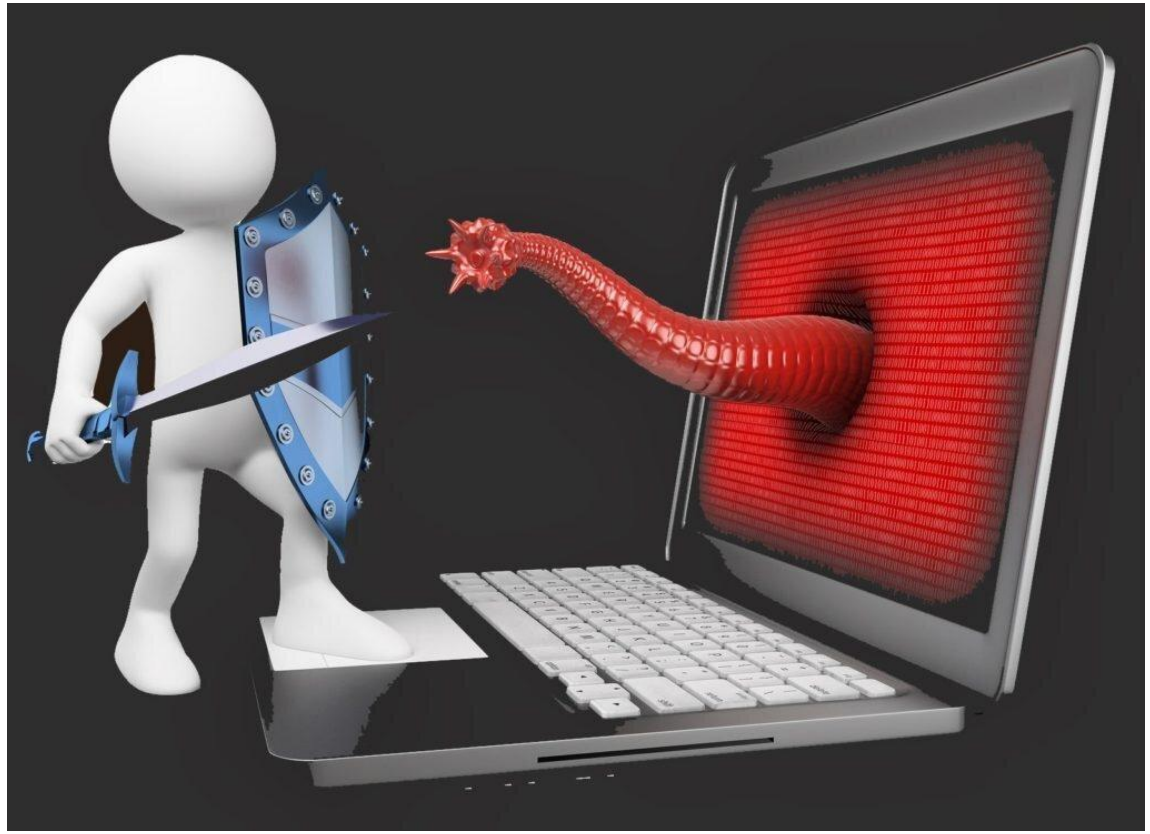


Рис.2 Угрозы информационной безопасности

Методы защиты

ПОЛИТЕХ

Организационные меры:

- Разработку политики информационной безопасности
- Контроль доступа к информации
- Обучение персонала
- Управление инцидентами
- Сертификацию и лицензирование

Технические меры:

- Межсетевые экраны (файрволы)
- Системы обнаружения и предотвращения вторжений (IDS/IPS)
- Криптографические средства
- Физические средства защиты
- Модули доверенной загрузки

Программные меры:

- Антивирусы и антишпионские программы
- DLP-системы (Data Loss Prevention)
- SIEM-решения (Security Information and Event Management)
- EDR (Endpoint Detection and Response)
- VPN (Virtual Private Network)

Дополнительные методы:

- Резервное копирование данных
- Токенизация
- Обфускация данных
- Многофакторная аутентификация (MFA)
- Аудит безопасности

Информационная безопасность в повседневной жизни

Важно обращать внимание на следующие пункты:

1)Защита личных данных

2)Безопасность в социальных сетях

3)Надежные пароли

4)Информационная безопасность в бизнесе

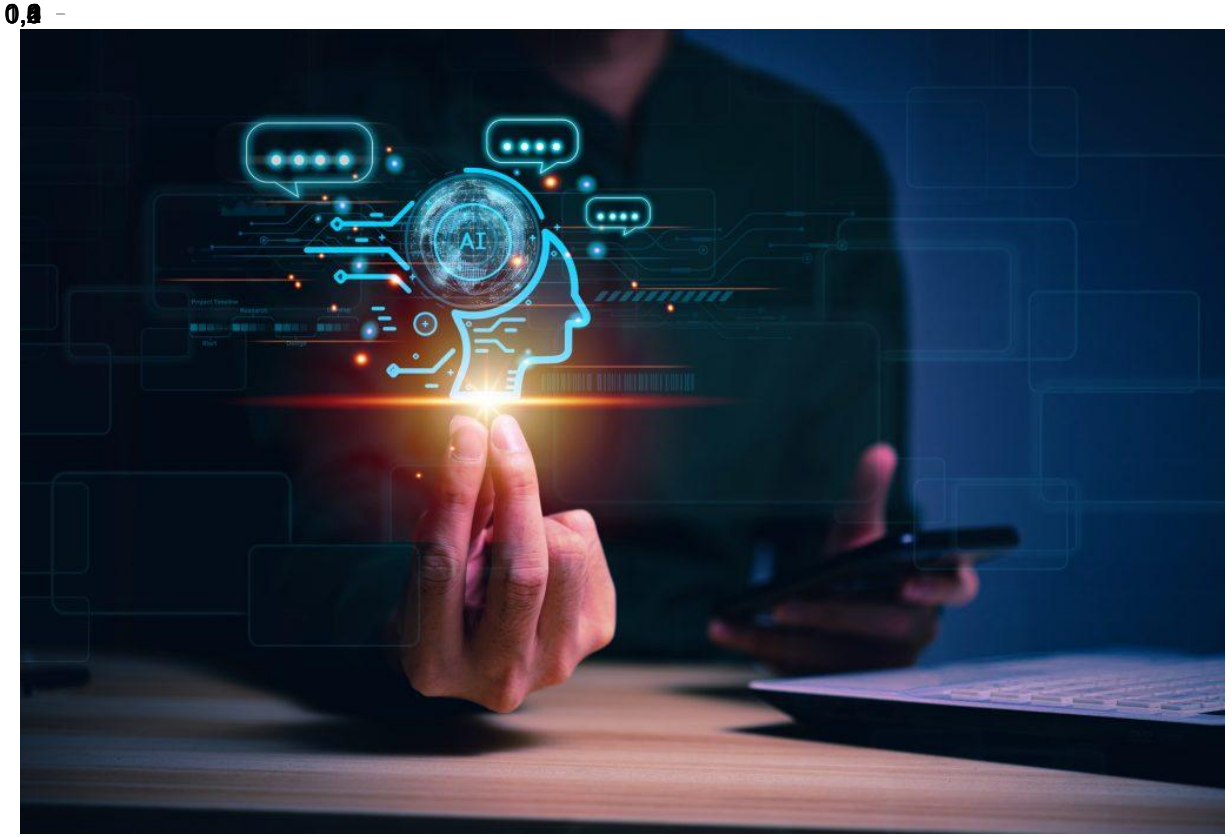


Рис.3 Информационная безопасность в повседневной жизни

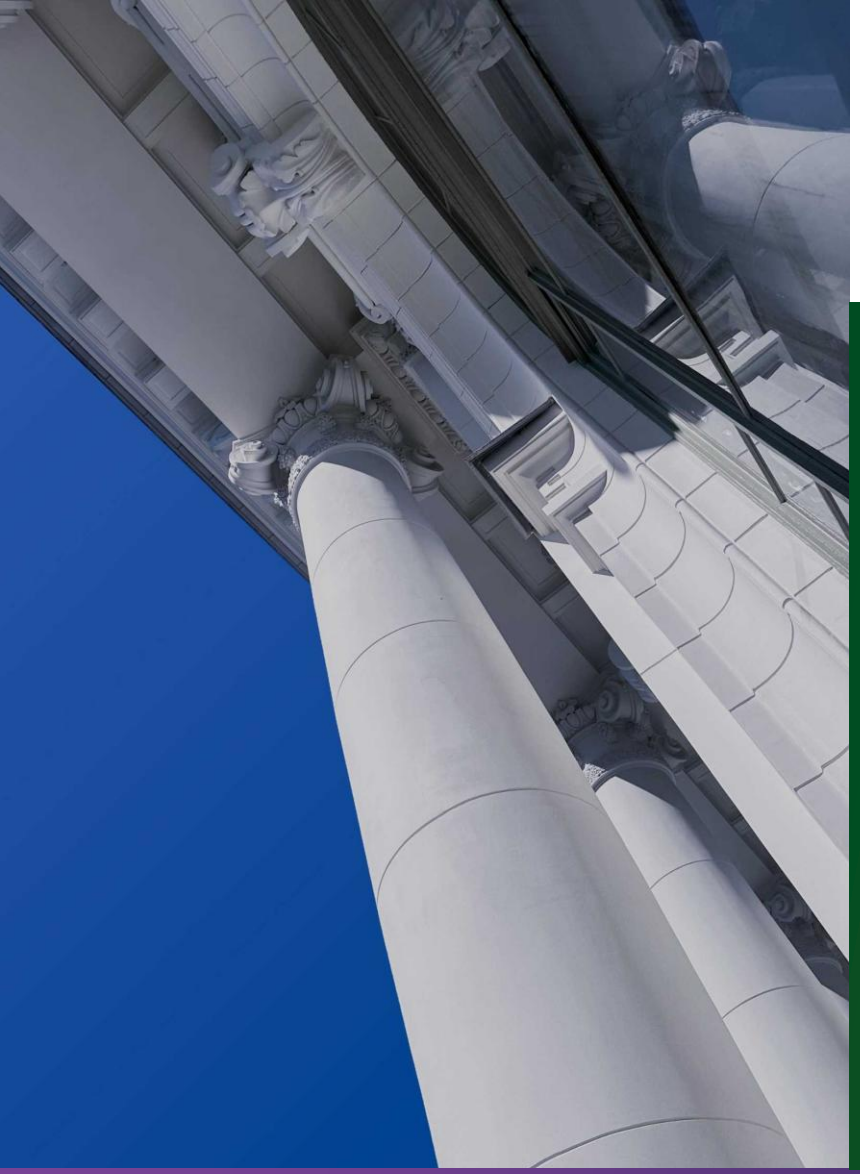
Законодательство в сфере информационной безопасности

ПОЛИТЕХ

В России защита данных регулируется двумя законами. Они касаются персональных данных и критической инфраструктуры:

- 152-ФЗ «О персональных данных» — главный российский закон по защите личной информации. Он требует шифровать персональные данные и сообщать об утечках.
- 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» — описывает требования к безопасности банков и энергетики.

Рис.5 Федеральный закон «О персональных данных»



Вывод

В современных условиях угрозы информационной безопасности представляют собой сложную систему взаимосвязанных рисков, требующих комплексного противодействия. Как показывает анализ, эффективная защита не может ограничиваться техническими решениями - необходимо создание целостной системы, объединяющей три критически важных компонента: передовые технологии, регламентированные процессы и, что особенно значимо, осознанное поведение каждого пользователя. Именно такой многоуровневый подход позволяет сформировать устойчивую культуру кибербезопасности, способную адаптироваться к постоянно эвол

ПОЛИТЕХ

Источники информации

1. https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/sredstva-obespecheniya-ib/tekhnicheskie-i-programmnye-sredstva-informatsionnoj-bezopasnosti/
2. https://developers.sber.ru/help/business-development/infrastructure-security
3. https://kedu.ru/press-center/articles/info-information-security-metody-obespecheniya/#ancr1
4. https://skillbox.ru/media/code/informacionnaya-bezopasnost/