ЧПОУ "СККИТ"

Информационные и телекоммуникационные технологии в профессиональной деятельности

Две опоры профессионала: компьютерные сети и интернет как инструмент работы — и информационная и техническая безопасность как условие доверия к этому инструменту.

ВОЗМОЖНОСТИ ИКТ

Что дают ИКТ-технологии профессионалу: пять ключевых возможностей

01

Удалённый доступ к рабочим системам

Подключение к корпоративной сети из дома или командировки: бухгалтер открывает 1С через VPN, инженер — SCADA-панель цеха.

02

Электронный документооборот и облака

Договоры и акты подписываются ЭЦП за минуты, а файлы хранятся в облаке и доступны всей команде без бумажной волокиты.

03

Онлайн-коммуникации и видеоконференции

Совещание с филиалами в другом городе без перелёта: видеозвонок, общий экран и запись встречи для отсутствующих.

04

Автоматизация расчётов и аналитики

Таблицы, ERP и BI-отчёты считают смету или план продаж за секунды — специалист тратит время на решения, а не на рутину.

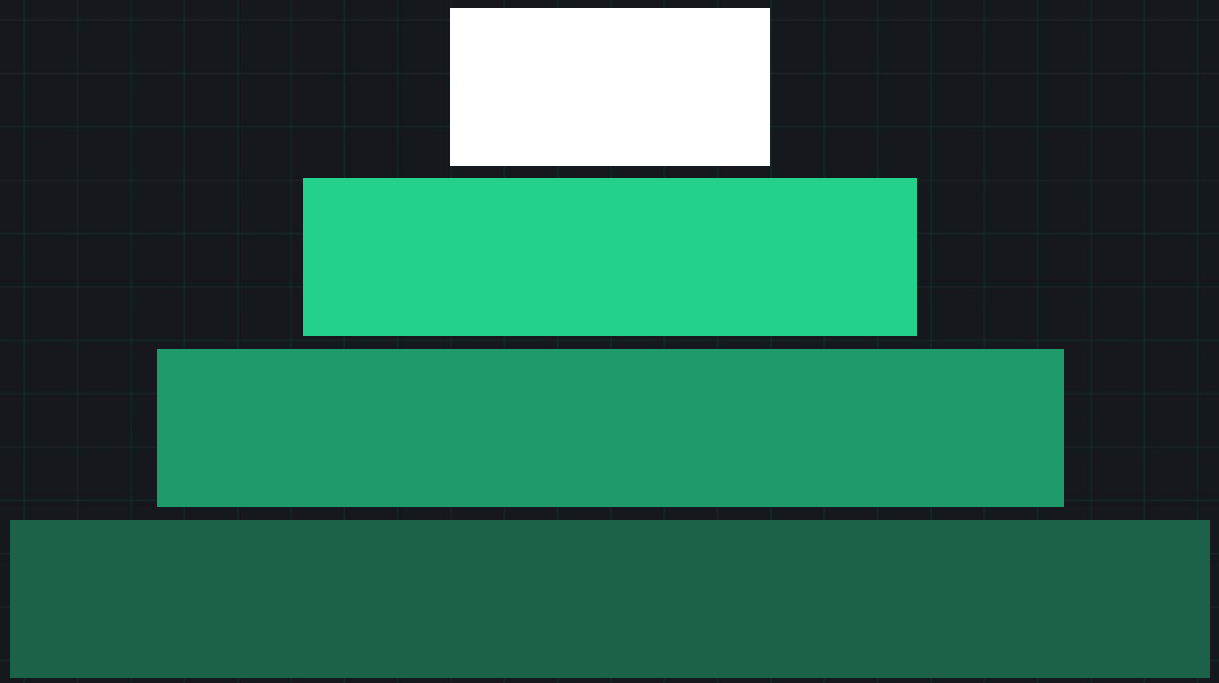
05

Дистанционное обучение и курсы

Курсы, вебинары и электронные библиотеки позволяют осваивать новую профессию или стандарт без отрыва от работы.

КЛАССИФИКАЦИЯ СЕТЕЙ

Компьютерные сети: от локальной к глобальной



PAN — персональная

До 10 м: Bluetooth, USB, наушники, смарт-часы

LAN — локальная

Офис/здание: десятки устройств, коммутатор, сервер

MAN — городская

Город: провайдеры, корпоративные каналы, ЦОД

WAN — глобальная

Интернет: маршрутизаторы, магистрали, страны

СЕТИ И ИНТЕРНЕТ

Как работает интернет: модель TCP/IP и путь пакета

1

Уровни TCP/IP: от канала до приложения

Канальный (Ethernet, Wi-Fi) — кадры в локальной сети. Сетевой (IP) — адресация и маршрутизация. Транспортный (TCP/UDP) — доставка. Прикладной (HTTP/HTTPS, DNS) — сервисы.

2

Запрос: имя → DNS → IP-адрес

Браузер шлёт доменное имя на DNS-сервер и получает IP-адрес. Затем устанавливает TCP-соединение; для HTTPS — TLS-рукопожатие и шифрование канала.

3

Маршрутизация и ответ сервера

Пакеты идут через маршрутизаторы по таблицам маршрутизации. Сервер обрабатывает запрос и возвращает ответ: TCP подтверждает доставку, HTTP/HTTPS передаёт данные.

КОМПЬЮТЕРНЫЕ СЕТИ И ИНТЕРНЕТ

Интернет в 2026 году: технологии доступа и ключевые тренды

5G

Мобильный доступ

Массовое развёртывание, обсуждение 6G

Спутник

Широкополосный доступ

Связь в удалённых и труднодоступных районах

Облака

Сервисы и вычисления

Рабочие сервисы и хранение данных

IoT

Подключённые устройства

Датчики, оборудование, умные системы

Web3

Новая архитектура веба

Децентрализация и распределённые сервисы

ИИ-сервисы

Драйвер трафика и угроз

Генеративные модели в работе и атаках

Проводной доступ — скорость и стабильность,

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность: что защищаем и от кого

S Сильные стороны: триада Ц-Ц-Д

Конфиденциальность — данные доступны только тем, кому положено

целостность — защита от искажения

доступность — сервис работает, когда нужен

W Слабые места

Человеческий фактор и социальная инженерия

устаревшее ПО и незакрытые уязвимости

слабый контроль доступа и резервного копирования

O Возможности

Многофакторная аутентификация, шифрование, регулярные бэкапы, обучение сотрудников, мониторинг и SIEM, ИИ-аналитика угроз

T Угрозы

Вредоносное ПО и программы-вымогатели, фишинг, утечки данных, внутренние нарушители

ответственность по 152-ФЗ и 149-ФЗ

ЛАНДШАФТ КИБЕРУГРОЗ

Киберугрозы 2026: масштаб и статистика

74%

Утечек — персональные данные

Доля всех утечек в России, 2025

4,5 млрд

Записей персональных данных

Утекло из российских компаний за 2023–2025

32,3%

Утечек — коммерческая тайна

Доля инцидентов, 2025

10%

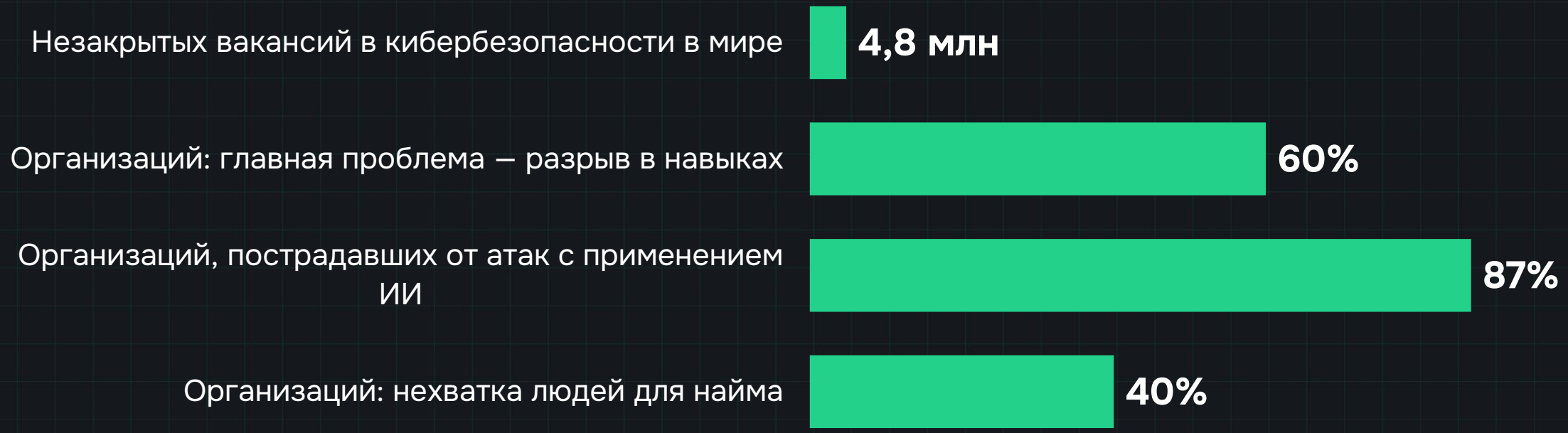
Случайные утечки через облака

Рост доли инцидентов, 2025

Россия — среди мировых лидеров по публичным утечкам; драйвер атак — ИИ

Источник: ЭАЦ ГК InfoWatch, отчёт об утечках за 2025 год

ИИ в атаках и в защите: двойная роль технологии



Разрыв в навыках (60%) впервые обогнал нехватку персонала (40%): защите нужны не головы, а компетенции.

SANS | GIAC, 2026 Cybersecurity Workforce Research Report (947 респондентов); Cybersecurity Guide, 2026

ТЕХНИЧЕСКАЯ ЗАЩИТА

Уровни технической компьютерной безопасности

Уровень 1 СЕЙЧАС

Физический: контроль доступа к оборудованию, охрана серверных, замки и пропуска

Уровень 2 СЕЙЧАС

Сетевой: межсетевые экраны, VPN, сегментация сети

Уровень 3 СЕЙЧАС

Хостовый: антивирус, EDR-системы, своевременные обновления

Уровень 4 СЕЙЧАС

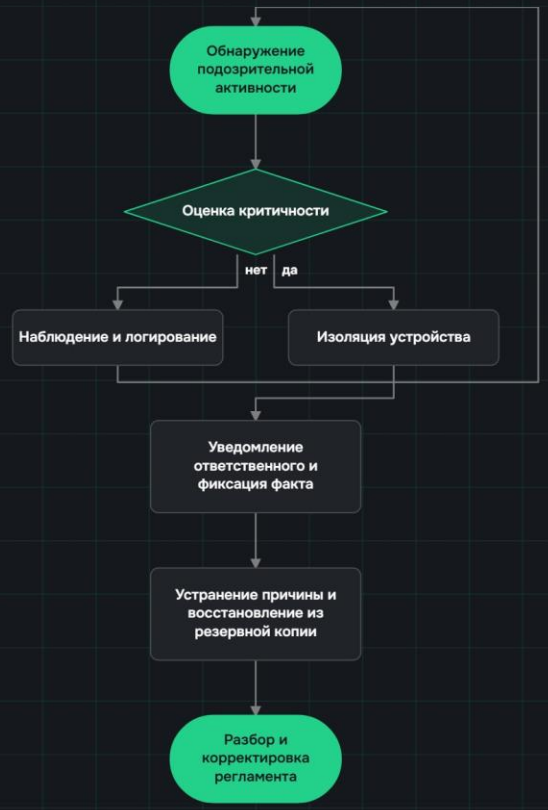
Прикладной: шифрование данных, многофакторная аутентификация

Уровень 5 СЕЙЧАС

Организационный: регламенты, политики, резервное копирование

РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

Алгоритм действий при инциденте информационной безопасности



Ветка «нет» возвращает к мониторингу; ветка «да» ведёт к полному циклу реагирования.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Правила безопасной работы: чек-лист для сотрудника

Семь привычек, которые закрывают большинство типовых рисков — от утечки пароля до заражения через вложение.

- **Уникальные сложные пароли в менеджере паролей**
- **Многофакторная аутентификация на почте, VPN и рабочих аккаунтах**
- **Своевременные обновления ОС и прикладного ПО**
- **Проверка отправителя и домена перед ответом или переходом по ссылке**
- **Никаких личных флешек и сторонних носителей на рабочем ПК**
- **Блокировка экрана при отходе от рабочего места**
- **Резервные копии данных и немедленное сообщение об инциденте в службу ИБ**

ФИНАЛ

Спасибо за внимание!

ИКТ дают скорость и мобильность — но безопасность остаётся процессом и культурой.