Развитие приложений и сервисов, которыми мы пользуемся, базируется на множестве разных технологий. Постоянно появляются новые устройства, новые способы хранения и обработки данных, увеличиваются вычислительные мощности устройств.

При этом с развитием технологий появляется всё больше **угроз и проблем,** например:

- безопасность данных;
- сложности с хранением и обработкой информации (потому что информации генерируется всё больше);
- сложно быстро адаптироваться к постоянно изменяющимся условиям.

В этом юните мы разберём, какие технологии в данный момент активно развиваются и имеют большой потенциал, и как они могут решить проблемы, которые существуют в мире IT.

Большие данные (Big Data)

Big Data — это технология обработки больших объёмов информации.

Это могут быть миллиарды и триллионы записей из различных источников, часто никак не структурированные. Такие объёмы данных невозможно обработать привычными методами, поэтому специалисты по Big Data разрабатывают особые методы сбора, обработки и хранения таких данных.

Какие данные это могут быть?

В качестве примеров можно привести данные из соцсетей, информацию о покупках в Интернет-магазинах, метеорологические данные с разных точек планеты, информацию о банковских операциях и т.д. Эта информация предоставляет огромную ценность для различных заинтересованных лиц (компании, государство, аналитики).

Суть анализа больших данных состоит в поиске закономерностей, которые позволят сделать определённые выводы и предсказать возможное развитие событий (например, погоду, пробки на дорогах, изменения в покупательском поведении), отследить различные тренды в обществе и в экономике.

Направления

В сфере Big Data существует два основных направления:

→ **Big Data engineering**

→ **Big Data analytics**

Специалисты по Big Data engineering занимаются тем, что проектируют системы для сбора, хранения и обработки данных, в то время как Big Data аналитики занимаются тем, что интерпретируют собранные данные: ищут закономерности и тенденции, классифицируют информацию и делают на её основе различные прогнозы.

Один из бесплатных сервисов, основанных на Big data — Google Trends. В нём собрано огромное количество данных по запросам в Google от пользователей с разных стран мира. Вы можете попробовать себя в роли аналитика больших данных и попробовать найти интересные тенденции и закономерности в какой-либо интересующей вас теме.

Например, если запросить статистику по запросу Game of Thrones (т.е. сериал «Игра Престолов»), на графике мы увидим несколько пиков — вспышек интереса, которые совпадают с выходами новых сезонов сериала.

Облачные технологии

Облачные технологии — это технологии распределённой обработки данных, в которых компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Вычислительные мощности (например, приложения или базы данных) располагаются на внешних серверах (другими словами, «в облаке»), и вам достаточно подключиться к внешнему серверу, чтобы воспользоваться этими вычислительными мощностями.

Облачные технологии сейчас распространены повсеместно и сильно упрощают жизнь как обычным пользователям, так и бизнесам различного уровня. Например, если раньше для того, чтобы пользоваться почтой,

вести бухгалтерию, обрабатывать фото или видео, вам нужно было скачивать на свой компьютер специальное ПО, сейчас в этом нет необходимости. Многие сервисы теперь располагаются в облачных хранилищах, и вы можете воспользоваться ими с любого устройства через браузер или через специальное приложение, если речь идёт о телефоне.

Большинство из нас постоянно пользуются облачными технологиями, даже не задумываясь об этом: **Dropbox, Google-документы, Skype, WhatsApp, Microsoft Office** — это лишь небольшой список продуктов, которыми мы пользуемся каждый день и которые основаны на использовании облачных серверов.

☆ Преимущества облачных технологий

«Облачный» подход даёт множество преимуществ:

- **Вы не зависите от вычислительных мощностей своего устройства.** Большинство ресурсозатратных операций происходит на удалённом сервере, а на клиенте (т.е. на вашем устройстве) вы видите уже конечный результат этих операций.
- **Нет необходимости заботиться о бэкапах данных.** Если с вашим телефоном или компьютером что-то случится, то ваши данные (почта, переписки, фотографии, документы), которые хранились в облаке, не пострадают. Вы сможете легко получить к ним доступ с другого устройства.
- **Возможность организации общего доступа к информации.** Благодаря облачным серверам, вашу информацию могут просматривать и редактировать любые пользователи, которым вы предоставите доступ.
- **Безопасность и надёжность**. Все заботы по организации работы серверов и сохранность данных ложатся на поставщика услуг, у которого, как правило, имеются в распоряжении мощные ресурсы, чтобы обеспечить бесперебойность работы и защиту от взломов.

⊖ Слабые стороны облачных технологий

Приложения на основе облачных вычислений, как правило, имеют следующие слабые стороны:

- **Стабильное подключение.** Пользователь облачного сервиса во многом зависит от постоянного и стабильного Интернета.

- **Защита данных.** Ваши личные данные (включая конфиденциальную информацию) будут храниться на серверах компании-поставщика. Несмотря на то, что это, как правило, надёжнее, чем хранить данные на личном ПК, не существует ни одной компании, которая могла бы гарантировать вам 100% защиту данных. Даже серверы таких гигантов, как Google или Amazon, иногда страдают от атак хакеров.

Интернет вещей

Под **Интернетом вещей** понимается сеть, объединяющая различные устройства вокруг нас. Сюда относятся не только уже привычные нам смартфоны и ноутбуки, но и целый ряд других «умных» устройств — часы, холодильники, тостеры, пылесосы, камеры видеонаблюдения и так далее, т.е. те устройства, которые имеют выход в Интернет.

Источник: fierceelectronics.com

Интернету вещей можно противопоставить «Интернет людей», то есть всю совокупность людей, имеющих выход в интернет. Интересно, что в 2009 году количество устройств, подключенных к Интернету, превысило количество людей. Уже сегодня к Интернету подключено более 20 миллиардов различных устройств.

☆ Какие преимущества могут дать нам такие технологии?

→ Удобство

Не зря говорят, что лень — двигатель прогресса. Уже сейчас появление умных устройств сильно упрощает нам жизнь. С помощью смартфона или компьютера мы можем управлять роботами-пылесосами, различной кухонной техникой, настраивать освещение в доме и многое-многое другое.

→ Безопасность

В данном случае речь идет даже не столько о различных системах видеонаблюдения и контроля доступа, которые уже распространены

повсеместно. Уже существуют разработки специальных датчиков, которые отслеживают состояние мостов и дорог и сообщают специалистам о возможных проблемах: например, подземные толчки, или наледь на дороге, чтобы они успели решить её до возникновения несчастных случаев.

→ **Здоровье**

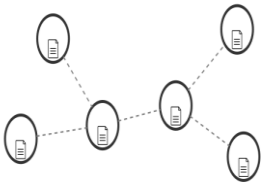
Различные фитнес-трекеры и браслеты уже умеют отслеживать пульс и показатели качества сна. В данный момент ведутся работы над ещё более современными технологиями: чипы для автоматического контроля уровня сахара в крови или артериального давления. Это могло бы помочь людям, находящимся в группе риска по здоровью (например, диабетики или гипертоники), лучше заботиться об организме и принимать своевременные меры в случае возникновения проблем.

Blockchain

Технология блокчейн имеет стойкую ассоциацию с криптовалютами, потому что она была использована при создании первой криптовалюты — биткоина — и прославилась вместе с ним.

Но на самом деле **блокчейн** — это просто технология хранения и передачи данных, которая может быть использована в различных сферах.

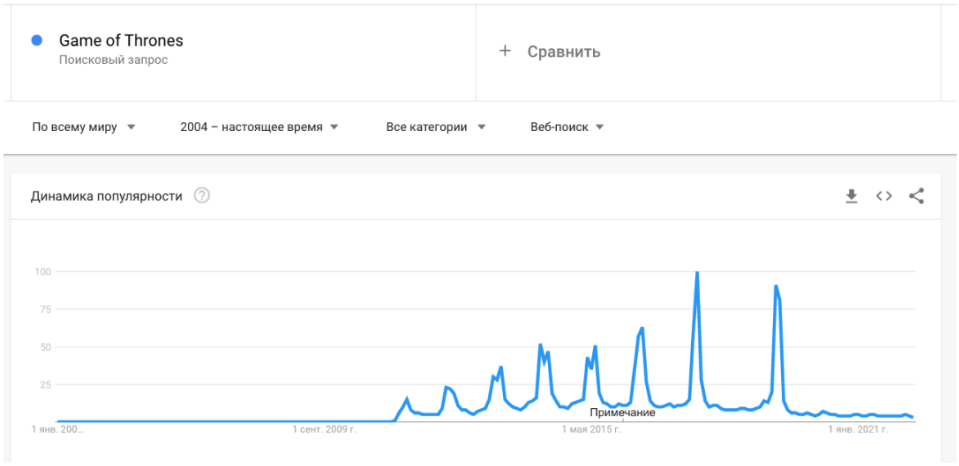
Представьте, что у вас есть записная книжка, куда вы записываете свои расходы и доходы: потратил 100 рублей в магазине, получил зарплату, заплатил за такси. Чтобы посторонний человек не мог внести записи в вашу книжку, вы используете шифрование, причем шифр известен только вам. Кроме того, вы не храните записную книжку в одном экземпляре, ведь с ней может что-то случиться — потеряли или украли. Поэтому у вас есть несколько экземпляров, которые вы храните в разных местах. При внесении новых записей проводится проверка, что изменения внесли именно вы, после чего данные обновляются во всех копиях книжки.



Источник: neo4j.com

Примерно так устроена технология блокчейн:

- По своей сути это **база данных**, информация в которой организована в виде блоков. Каждый из этих блоков содержит зашифрованную часть информации, а также ссылку на предыдущий блок и метку времени.
- Новые блоки всегда добавляются в конец цепочки. Вставить новый блок между двумя уже имеющимися или **подменить информацию невозможно**, потому что ссылки на блоки и хронологические метки не будут соответствовать друг другу, и система не пропустит такие правки.
- Поскольку все данные зашифрованы, вносить информацию могут только **доверенные лица** — те, у кого есть специальный ключ.
- Кроме того, блокчейн не имеет общего сервера — данные распределены на множестве устройств. Благодаря этому **информация остаётся открытой и всегда актуальной** для всех её пользователей.



Задание 4.10.1

1/1 point (ungraded)

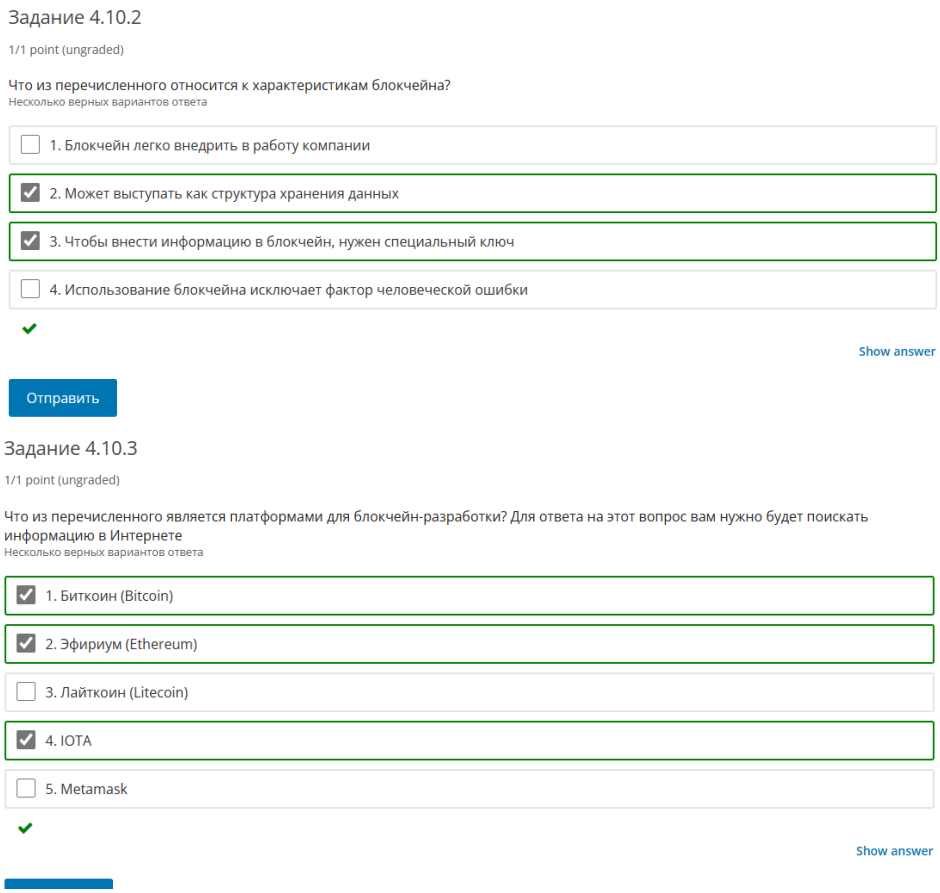
Зайдите на сервис Google Trends по ссылке выше и проанализируйте статистику по запросу «Big Data» во всём мире за период с 2004 года по настоящее время. Пользуясь графиком, определите, в каком году был зафиксирован самый высокий интерес к термину Big Data?

Примечание. В ответе впишите только год. Если пиковых точек несколько, впишите любую из них.

2017 ✔

2017

Z



Сферы применения блокчейна

Блокчейн активно применяется в различных сферах:

- **Финансовые и юридические операции.** В этих сферах безопасность сделок имеет особо важное значение. С помощью блокчейн можно осуществлять подтверждение личности, заключение различных контрактов и договоров.
- **Медицина**. Некоторые медицинские учреждения начинают переводить базы данных на систему блокчейна. Это позволит избавиться от вечной проблемы медицинских учреждений: когда теряются карты пациентов, данные об анализах, обследованиях и т.д.
- **Голосование**. Блокчейн может решить основные проблемы с голосованием: исключить подтасовки и фальсификации. В Эстонии уже в 2016 году провели первые испытания голосования на основе блокчейна.
- **Логистика.**
- **Авторское право.**

Задание 4.10.4

1/1 point (ungraded)

Представьте, что вы проектируете приложение — виртуальную примерочную. Приложение должно работать следующим образом: пользователь загружает фото в полный рост, фото обрабатывается приложением и появляется возможность примерить одежду из ассортимента магазина прямо на фотографии.

Какие из этих технологий вы бы вероятнее всего использовали?
Несколько верных вариантов ответа

- [x] 1. Облачные технологии
- [ ] 2. Блокчейн
- [x] 3. Дополненная реальность
- [x] 4. Искусственный интеллект

✔

Ответ
Верно:
1 – верно! Фото будет загружаться и обрабатываться в облаке.
3 — верно! Существующий виртуально объект — модель одежды — будет накладываться на реальную фотографию пользователя.
4 — верно! ИИ понадобится для того, чтобы «подогнать» одежду под реальную фигуру пользователя, и конечный результат примерки выглядел правдоподобно.

Show answer

Задание 4.10.5

1/1 point (ungraded)

Необходимо разработать приложение для компании, которая занимается поставками грузов. Приложение должно собирать данные с различных датчиков, установленных на машинах: количество используемого топлива, состояние шин и двигателя, информацию с GPS-трекеров. Эти данные используются для оптимального управления автопарком, например, они помогают предсказать, когда машину нужно отправить на техосмотр или ремонт, или когда нужно подобрать для дальних перевозок более надёжный транспорт.

Какие из этих технологий вы бы вероятнее всего использовали?
Несколько верных вариантов ответа

- [x] 1. Big Data
- [ ] 2. Облачные технологии
- [x] 3. Искусственный интеллект
- [x] 4. Интернет вещей
- [ ] 5. Блокчейн

✔

Ответ
Верно:
1 — верно! Для анализа большого количества различных данных понадобятся методы Big Data.
3 — верно! ИИ будет отвечать за анализ данных с датчиков и определение состояния автопарка, подбор наилучшего транспорта для поездки.
4 — верно! Датчики на машинах, отправляющие данные на сервер, являются примером интернета вещей.

Show answer

Отправить

Задание 4.10.6

1/1 point (ungraded)

Представьте, что вы руководитель стартапа, который разрабатывает систему, которая на основании анализа постов в соц. сетях будет анализировать мнение населения о политиках и предсказывать результаты выборов в стране.

Каких специалистов вы бы набрали в свою команду?

Несколько верных вариантов ответа

- [x] 1. Специалист по Big Data
- [x] 2. Business Intelligence аналитик
- [x] 3. Специалист по машинному обучению
- [ ] 4. Маркетолог

✔

Show answer

Отправить

Задание на mind map

Нанесите на ментальную карту области, с которыми вы познакомились в этом юните.

1. Для Big Data укажите:

- какие задачи решает эта сфера;
- какие 2 направления в ней можно выделить;
- какие специалисты работают в сфере.

2. Для облачных технологий укажите:

- какие проблемы решает применение облачных технологий;
- какие виды облачных сервисов по типу предоставляемых услуг существуют (эту информацию вам нужно будет найти самостоятельно).

3. Для интернета вещей укажите:

- какие проблемы решает эта сфера;
- приведите 5 примеров устройств, относящихся к интернету вещей.

4. Для блокчейна укажите:

- какие проблемы решает использование блокчейна;
- в каких сферах используется эта технология.

DevOps

Про **DevOps** говорят и пишут уже больше 10 лет. При этом многие продолжают считать, что DevOps — это методология, профессия или конкретный набор инструментов.

На самом деле DevOps не является ни первым, ни вторым и никак не третьим. Это целая культура со своей философией. Благодаря внедрению DevOps в командах формируются процессы, повышающие эффективность бизнеса и усиливающие результат от социальных и технических нововведений.

DevOps-инженер — это специалист, понимающий все процессы цикла разработки продукта (разработку, тестирование, архитектуру, риски безопасности, подходы и средства автоматизации), а также оптимизирующий процессы в пред и пост-релизной поддержке продукта. Специалист выстраивает благоприятное сотрудничество между командами разработки и контролирует ожидания заказчика.

Философия DevOps строится на нескольких принципах:

- бережливое производство и гибкость;
- поток и цикличность процессов;
- прозрачность и безопасность;
- завершённость.

Рассмотрим подробнее принцип потока и цикличности, так как с жизненным циклом разработки ПО вы уже знакомы.

Принципы потока и цикличности

Так как DevOps подразумевает эволюционную трансформацию через обучение, этот процесс непрерывен. Поэтому в основе DevOps также лежат принципы потока и цикличности.

Поток означает непрерывность и сцепленность, цельность и взаимопроникновение процессов.

Это как две струи воды, которые смешиваются в одном стакане и образуют однородную жидкость. Вы будете часто встречать в описании DevOps такие вещи, как «поток ценности» — это создание новых характеристик продуктов, изменение, непрерывное улучшение. Движение без пауз. Конечно, иногда поток будет прерываться, как, например, поток реки, который что-то перегораживает. И вот тут будет важно собраться командой и решить: что перегородило ваш поток, как его устранить и стоит ли это вообще делать или достаточно пойти обходным путем. Как вы это сделаете — выбор за вами.

Циклы в DevOps есть везде:

- релизный цикл;
- жизненный цикл приложения;
- цикл изменений;
- цикл обсуждений;
- цикл тестирования.

Цикличность — неотъемлемая часть DevOps, так как именно циклы образуют те самые потоки создания ценности. Один цикл завершается и переходит в другой, чтобы всё началось с самого начала.

Продукт проходит цикл: от кода до релиза и непосредственной работы у пользователей, а затем возвращается на исходную точку в виде обратной связи от пользователей. Затем анализ, план и снова в работу.

Задание для DevOps-инженера

На примере портала Госуслуг и сервиса Яндекс.Такси (который мы анализируем) опишите сервис с точки зрения бережливого производства.

Попробуйте ответить на вопросы:

- Как вы понимаете принцип бережливого производства?
- Как в концепции порталов работает принцип бережливого производства?

Модель безопасности

Существуют разные схематические представления модели безопасности (пирамиды, колёса и т.д.). На рисунке ниже визуально представлена модель безопасности в виде пирамиды (**не путать** с security triangle).

Но мы рассмотрим модель в виде колеса **(infosec wheel)**, как более наглядную. Однако, блоки информации соотносятся друг с другом в обеих моделях.

Infosec wheel

Информационная безопасность организации, как правило, опирается на две команды специалистов **(пентестеров)**: **красную (red team)** и **синюю (blue team)**. Цветовое обозначение пошло ещё от американских военных, которые делились на две команды: красная —нападающие (или атакующие), синяя — защищающиеся (или обороняющиеся).

Их функции можно описать следующим образом: **red team** нападает извне, пытается всячески найти и проэксплуатировать уязвимости, а **blue team** строит всякие заборы, укрепляет сервисы и ставит ловушки на атакующих.

Разработчики также участвуют в развитии информационных систем организации, они постоянно пишут обновления системы и вводят их в эксплуатацию, а значит, открывают всё новое и новое поле для деятельности красной и синей команд. И в этих разработках нужно не забывать про безопасность.

Так появляются новые цвета в нашем «infosec wheel»: **жёлтый** (это сами разработчики), **зеленый** и **оранжевый** (это уже некий симбиоз безопасности с разработкой). И наиболее яркий пример этому — всё большая популярность специалистов DevSecOps (с 2018 года, до РФ вот как раз дошли тенденции).

DevSecOps — это важное направление в DevOps (наборе практик, нацеленных на взаимодействие разработчиков ПО с экспертами по безопасности), подразумевающее обеспечение безопасности на всех этапах разработки приложений.

Как показывает практика, организации, внедряющие безопасность в жизненный цикл ПО, демонстрируют лучшие результаты в обеспечении информационной безопасности. Подробнее можете прочитать в статье.

И тут возникает ещё больше направлений безопасности (помимо тестирования на проникновения и постройки заборов), а именно **статический** и **динамический анализы кода** и интеграция подходов безопасности в среду разработки. Это помогает избежать долгого и кропотливого тестирования уже готовой системы на выходе в эксплуатацию и постоянно на любом **билде** (версии или каких-то новых модулях системы) поддерживать высокий уровень безопасности.

Основная сложность при разработке чего-то нового или расширении возможностей существующей системы — это балансировать между безопасностью, функциональностью и простотой интерфейса.

Для сохранения такого баланса существует модель безопасности **security triangle** (треугольник безопасности) — условное представление состояния системы.

Если мы поставим точку внутри треугольника в любом месте (это будет маркер состояния нашей системы), то сможем соотнести уровни безопасности, функциональности и удобства пользования. Работает это так: чем ближе точка к security, тем ниже функциональность. Передвигая точку внутри треугольника, мы будем изменять состояние этих трёх параметров.

Например, мы хотим сделать банковское приложение, соответственно нам нужен максимально высокий уровень безопасности, и мы перемещаем точку в угол «security» — получаем максимальный уровень безопасности и никакой функциональности (кроме одной кнопки «Перевести деньги», например). И по потребительским качествам сервис будет низок. Чем больше мы добавляем плюшек и уходим в сторону функциональности, тем сложнее обеспечить безопасность и разобраться пользователю (как раз usability).

Infosec wheel затрагивает только «легальных безопасников», то есть специалистов профессионально занимающихся вопросами безопасности на основании договора (трудового или договора подряда, к примеру).

Но есть ещё одна классификация специалистов по безопасности (а именно хакеров), которая называет всех **шляпами (hat)** и делит также по цветам (белый, серый, черный).

Специалист по кибербезопасности

Чем же компьютерный «безопасник» отличается от хакера?

→ Хороший безопасник умеет пользоваться большим инструментарием взлома, более того, часто этим занимается, тестируя свою корпоративную сеть на уязвимости.

→ Любой хороший хакер по набору своих умений может быть безопасником, а безопасник — хакером. Это точно так же, как и полицейский, и бандит знают, где слепые зоны у камер наблюдения. Инструментарий у тех и других примерно один, просто применяется по-разному.

Кто такой хакер?

Какого-то общего определения не существует. Образовано это слово от английского *hack,* пришедшего к нам из сленга хиппи, и дословно обозначает «въехать» или «врубиться». В русской официальной

терминологии ещё используют слово «взломщик», но в реальной жизни, если сисадмин говорит «взломщик» — он чаще имеет в виду Бильбо Бэггинса.

Итак, можно сказать, что **хакер** — это человек, который ищет уязвимости в системе или сети, и использует их для собственной выгоды или развлечения.

Он может, например:

- написать вирус или троян (программу, дающую доступ в систему);
- подобрать пароль администратора;
- позвонить в бухгалтерию и, изобразив негодующее начальство, заставить работников совершить какую-то операцию, которая откроет для него доступ к данным;
- устроить DDoS-атаку — посылать огромное количество запросов к серверу, которое больше, чем его пропускная способность, а значит, на настоящие запросы от пользователей сервер отвечать уже не сможет.

Чем занимается специалист по компьютерной безопасности

Специалист по компьютерной безопасности старается не дать хакеру проникнуть в систему, получить выгоду или как-то покуражиться. Он защищает сеть от атак.

Иногда для этого он сам пытается взломать свои же серверы, тестируя их на отсутствие уязвимостей. Более того, есть целые фирмы **«этичных хакеров»** — это люди, которых за деньги нанимают, чтобы они взломали сеть предприятия и рассказали, как они это сделали, с целью устранить эту уязвимость.

Но гораздо чаще компьютерная безопасность (также её привыкли называть КБ) занимается базовой безопасностью, проверяя, нет ли очевидных уязвимостей.

Например, **инструмент nmap**, который может дать список всех открытых портов у всех компьютеров сети, — это стандартный тест безопасности, который в больших фирмах регулярно проводят.

Кроме того, специалист КБ обновляет все программы до самых актуальных стабильных версий, потому что в них устранены найденные свежие дыры в безопасности.

А ещё, что немаловажно, он разрабатывает **политику компьютерной безопасности компании** — свод правил, которым сотрудники должны следовать как в профессиональном поведении, так и в процессе настройки серверов.

Какого-то единого видения, как именно уберечь себя и компанию от хакеров, не существует. Специалист по безопасности разрабатывает такую политику для компании, где работает, на основе каких-то общеизвестных вещей, своих знаний и умений. Потому что мало ввести протокол безопасности, надо его ещё и поддерживать.

Кроме специалистов по компьютерной безопасности, есть ещё отдельная категория специалистов — **компьютерные криминалисты** или, как их ещё называют, **специалисты по компьютерной форензике** (от англ. forensics — криминалистика).

Компьютерные криминалисты, как правило, могут и взломать, и защитить систему, но их главная задача — исследовать последствия взлома. Они собирают все возможные сведения о том, как была совершена атака и ищут следы, которые оставили хакеры. И очень часто находят!

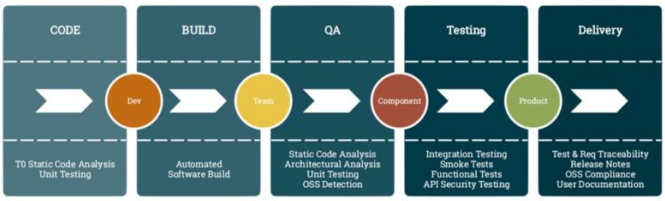
Но компьютерная форензика — это отдельная сложная дисциплина. Хотя и очень интересная.

Задание на mind map

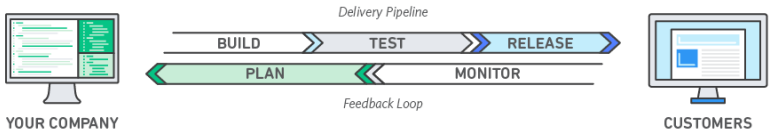
Изучите доступные дополнительные источники и добавьте на mind map **сферу девопс и кибербезопасности.**

Отобразите на карте следующую информацию:

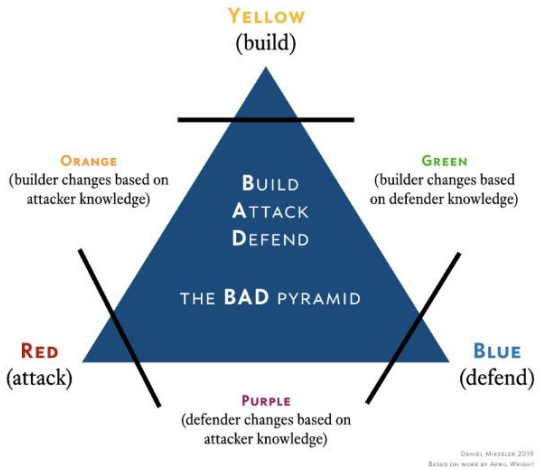
- задачи, которые решает девопс;
- задачи, которые решает кибербезопасность;
- специалисты, которые могут работать в этих сферах;
- отобразите на карте связи между этими сферами.



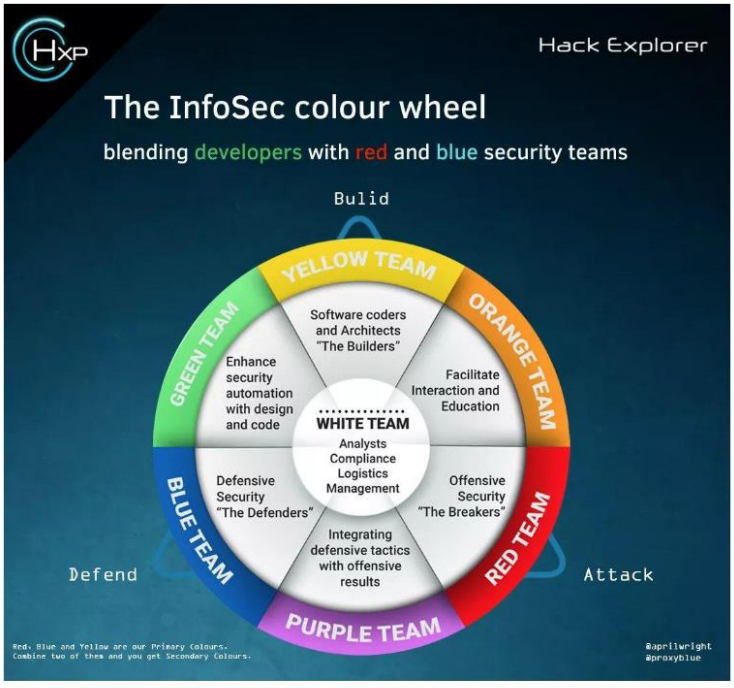
Пример потока разработки: от написания кода до доставки его на продакшн



Пример жизненного цикла ПО, взятый с сайта Amazon Web Services. Вы уже с ним знакомы



Infosec wheel



Модель безопасности infosec wheel. Источник: www.pinterest.co.uk

Задание 4.11.1

1/1 point (ungraded)

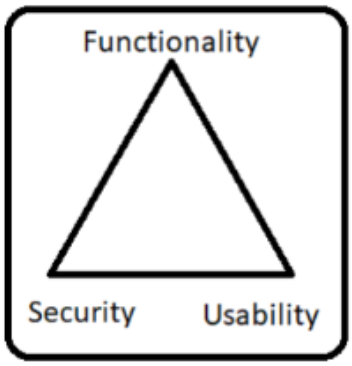
К деятельности каких пентестеров относится настройка межсетевых экранов и авторизации в сервисах?

- ○ red team
- ◉ blue team
- ○ yellow team

✔

Ответ
Верно: В их обязанности входит поддержание высокого уровня защищённости сервисов.

Show answer

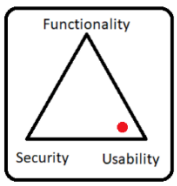


Security triangle. Источник: greycampus.com

Задание 4.11.2

1/1 point (ungraded)

Выберите верное утверждение, описывающее параметры системы по треугольнику безопасности:



- ◉ Низкий уровень безопасности, низкий уровень функциональности, высокая простота использования
- ○ Красная точка в сетевой инфраструктуре
- ○ Низкий уровень безопасности, большое количество разнообразных функций, минималистичный интерфейс с одной кнопкой
- ○ Низкая функциональность приложения, высокая защищенность системы, простой интерфейс для пользователя

✔

Ответ
Верно:
Судя по расположению точки в треугольнике безопасности, мы видим, что в этой системе може быть минимум функций, отсутствие шифрований, но её очень легко использовать, легкий, красивый и приятный интерфейс.

Show answer

Отправить

В данном модуле мы разобрали несколько важных сфер в IT, а именно:

- frontend-разработка;
- backend-разработка;
- сетевая инфраструктура;
- бизнес-аналитика;
- искусственный интеллект;
- Big Data;
- облачные технологии;
- Интернет вещей;
- блокчейн.

Кроме того, вы узнали, какие проблемы и какие потребности существуют в каждой из этих областей, а также какие специалисты в них работают. Эти знания помогут вам ориентироваться в трендах, понять, чем вам интересно заниматься, и найти своё место в мире IT.

Результатом работы над модулем стала ментальная карта IT сферы, к которой вы всегда можете обратиться, чтобы освежить свои знания, или при обдумывании нового проекта.

В следующих модулях вы начнёте погружаться в frontend-разработку!