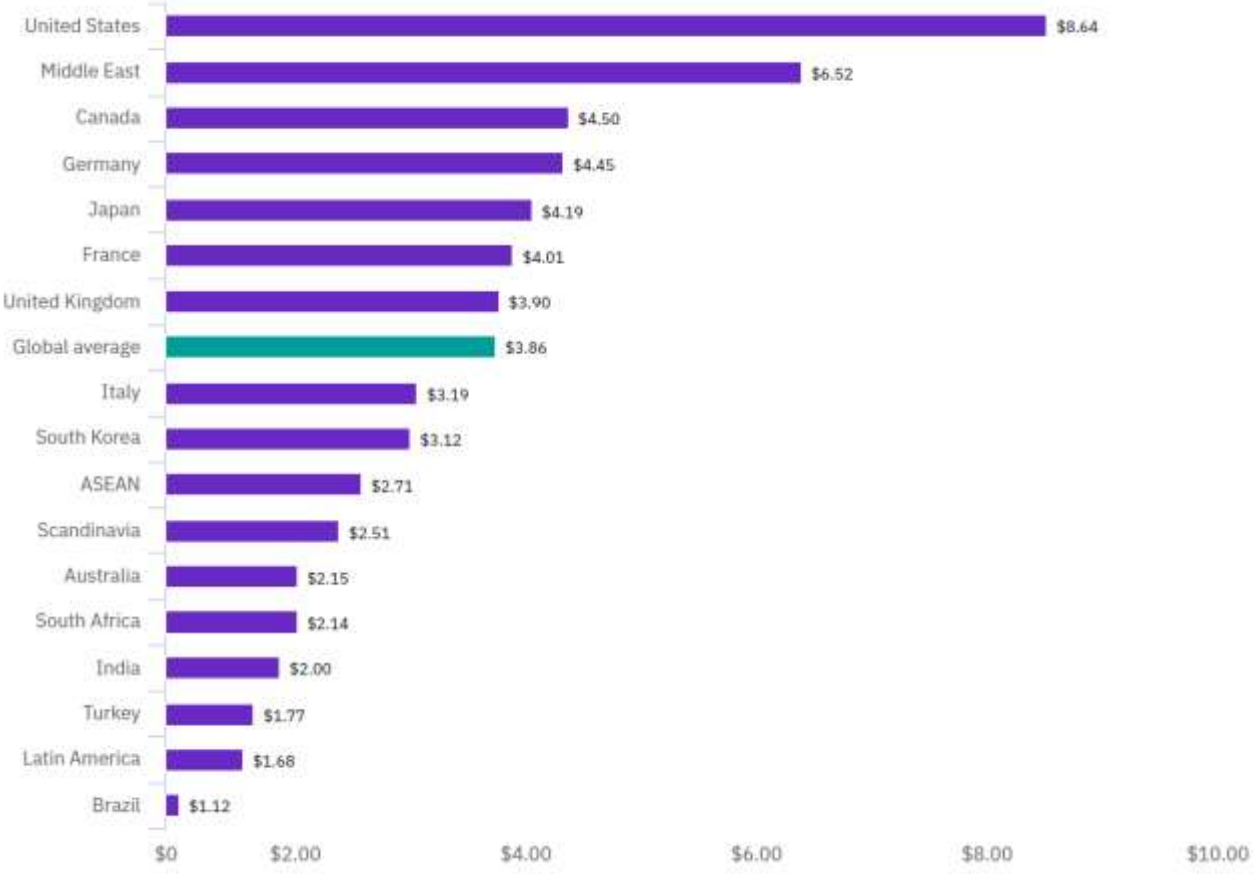
Место Киберполигонов в мире цифровых технологий

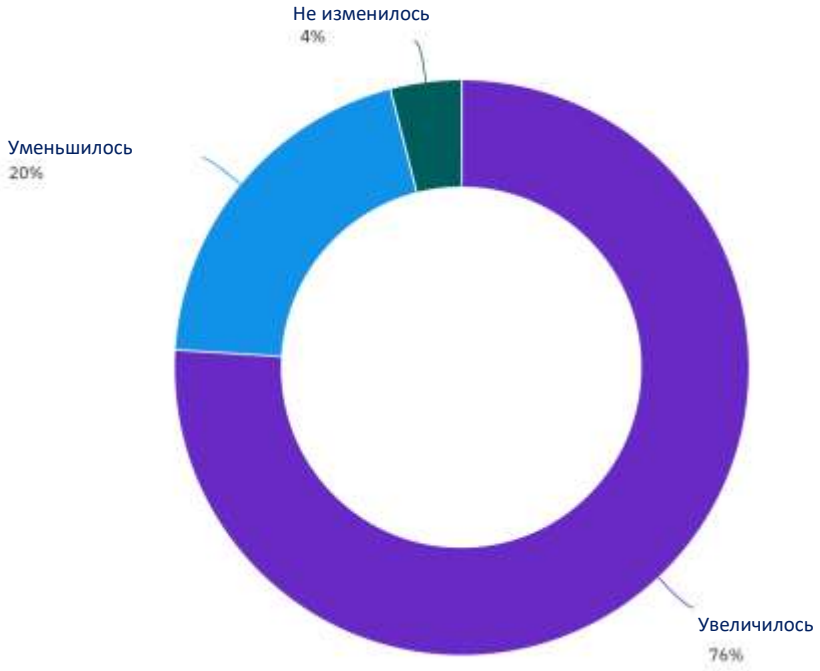
Средняя стоимость утечки данных (млн. USD)



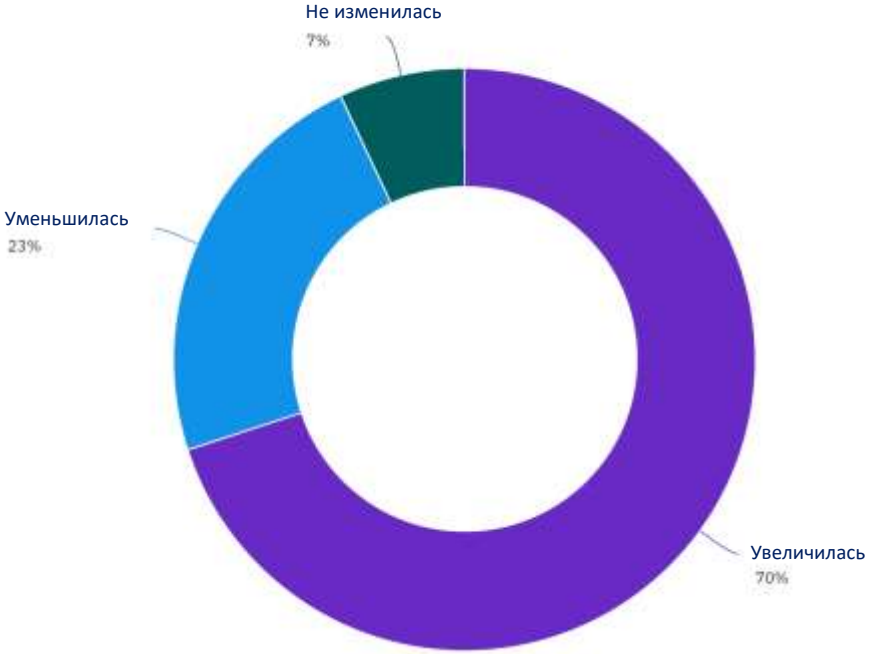
Source: ENISA

Влияние COVID-19 на кибер-риски

Время обнаружения проблем



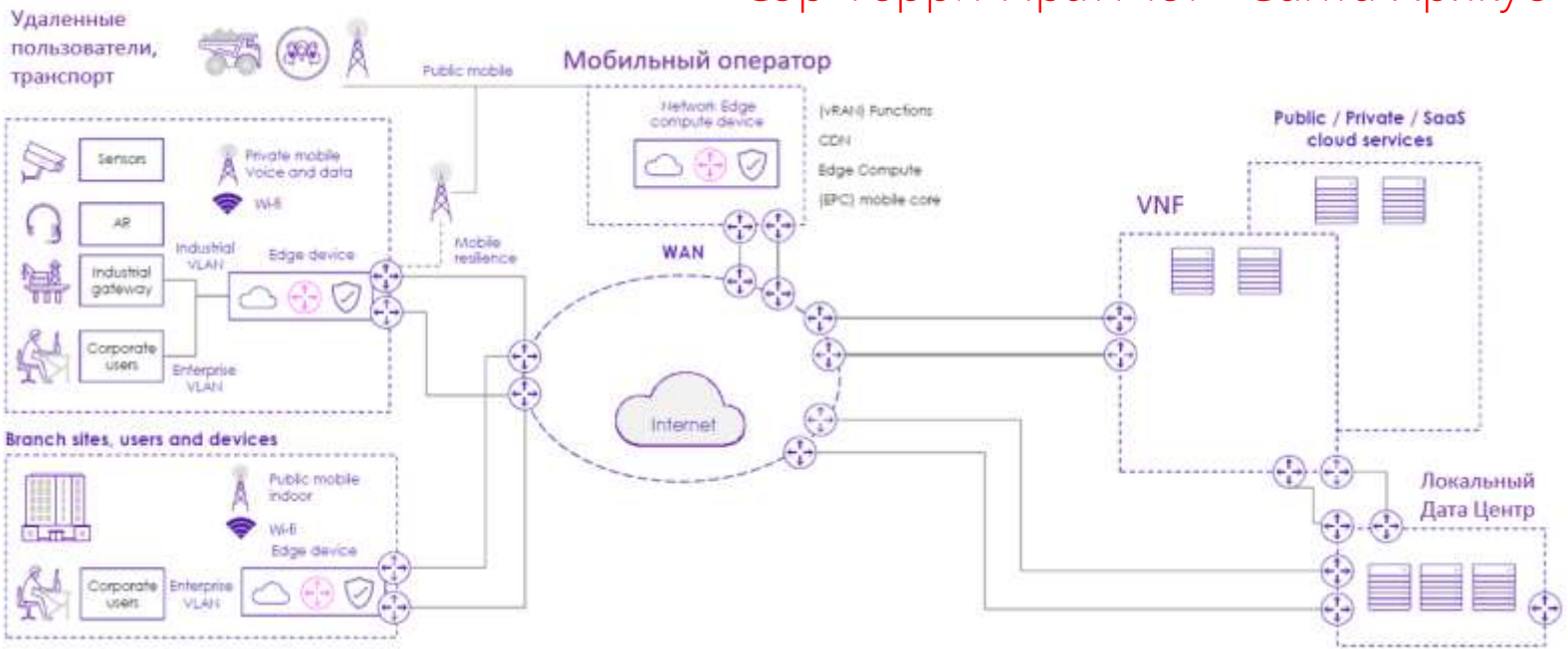
Средняя стоимость кибер-инцидента



Source: ENISA

Виртуальные киберпространства

«И тут декан произнес магическую фразу, на протяжении многих веков служившую двигателем науки и прогресса: – А почему бы нам не смешать все это и не посмотреть, что получится?»
Сэр Терри Праттчет «Санта Хрякус»



Текущие вызовы в телекоме

«Чтобы даже просто стоять на месте, нужно бежать со всех ног...»

Льюис Кэрролл "Приключениях Алисы в стране чудес".

- Взрывной рост использования новых технологий во всех отраслях экономики, требует от телеком-компаний стремительных действий по цифровой трансформации, не столько, чтобы достичь каких-то конкурентных преимуществ, сколько, как условие сохранения текущих рыночных позиций.
- Факторы риска:
  - конвергенция офисных и производственных сетей;
  - размывание периметра корпоративных сетей;
  - недостаток профильных специалистов ИБ.

Башни-близнецы

«— Хотелось бы мне, чтобы это случилось в другое время — не в мое.
— И мне бы тоже, да и всем, кто дожил до таких времен. Но выбирать не дано. Мы можем только решить, как распорядиться своим временем»
Д. Р. Р. Толкиен «Властелин колец»

Рик Рескорла

Ветеран вьетнамской войны Рескорла служил в ВТЦ главой охраны банка Morgan Stanley. Во время событий 11 сентября, благодаря ему спаслось около 2700 человек.

Недостаток кадров

“В мире не хватает более 200,000 специалистов по обеспечению кибербезопасности. К 2025 году дефицит таких специалистов составит 1,5 миллиона человек.”

Журнал Forbes, октябрь 2018

infotecs

Итоги крупнейшей телеком-аварии в истории США

В июне 2020 года в США произошла самая крупная в истории современного мобильного рынка авария на сети федерального оператора T-Mobile.

Случилась авария на одном из ключевых узлов магистральной сети. Из-за отсутствующего резервирования трафик попросту начал собираться в пробку, и на ее устранение ушло почти 13 часов. Федеральная комиссия по связи США только сейчас завершила свое расследование и делится полученными данными, позволяющими оценить масштаб телекоммуникационной катастрофы. Самым неприятным в этой истории стал тот факт, что более двухсот тысяч человек не смогли дозвониться в службу 911.

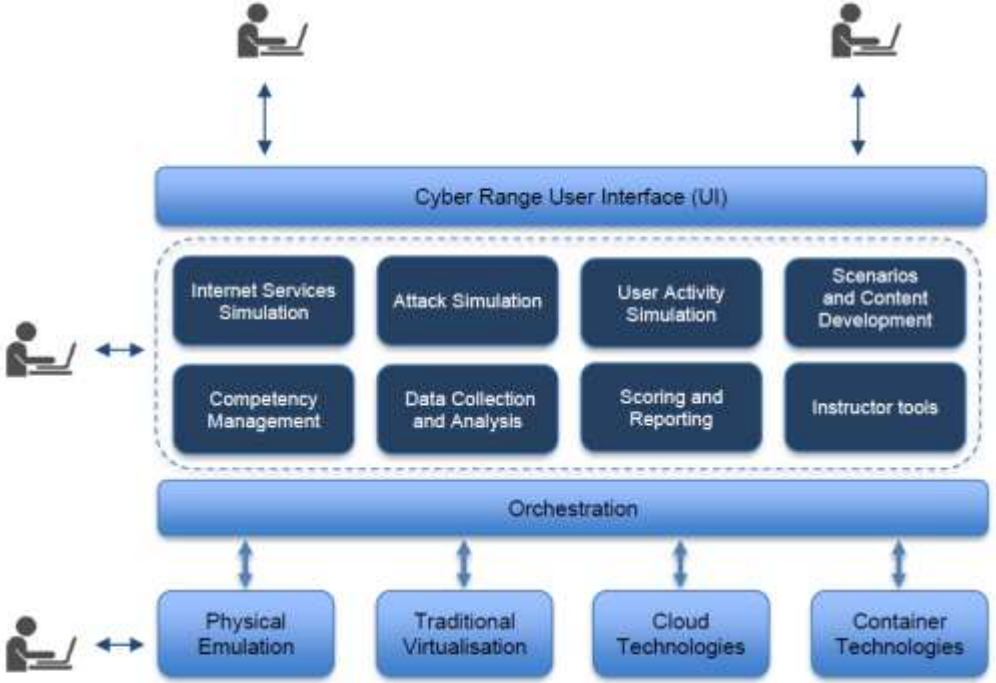
Оценки FCC неутешительные: 41% звонков, совершенных абонентами во время аварии, не увенчались успехом. При этом не учитывались звонки VoLTE и VoWiFi, из-за которых, к слову, и увеличивалась пробка из трафика в сети T-Mobile. Оператор же передал FCC данные лишь по звонкам, которые абоненты пытались совершать через сети 2G и 3G.

Что же касается входящих звонков, когда абоненты других операторов пытались дозвониться до абонентов T-Mobile, то по оценке FCC доля неудачных звонков в период аварии составляла 73%, это около 250 миллионов звонков. AT&T и U.S. Cellular сообщили, что не прошло 99% звонков на сеть T-Mobile, Verizon дал данные относительные — обычно неудачей заканчивалось около 100 звонков, тогда как в день аварии их количество достигло почти 12 миллионов.

Комиссия также выяснила, что аварию можно было устранить значительно быстрее, если бы инженеры T-Mobile правильно идентифицировали ее причины. В реальности действия инженеров оператора на первой стадии устранения аварии привели лишь к усугублению проблемы и возникновению кольцевой пробки. Отсутствие резервных каналов (как и собственных, ведь авария произошла на участке, который оператор арендует у сторонней компании) стала главной причиной случившегося.

Источник: Content-Review.com

Современные Киберполигоны (Cyber Range)



«Большое преимущество получает тот, кто достаточно рано сделал ошибки, на которых можно учиться»
Сэр Уинстон Черчилль

Технологии Киберполигона

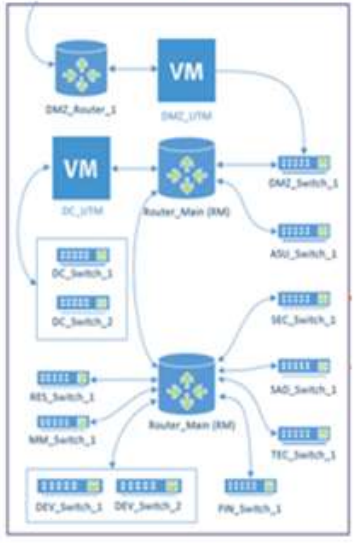
Функции Киберполигона

Source: Understanding Cyber Ranges

Ampire – российский вариант Cyber Range

«Единственный, кто поступал разумно, был мой портной. Он снимал с меня мерку заново каждый раз, когда видел меня, в то время как все остальные подходили ко мне со старыми мерками, ожидая, что я им буду соответствовать»
Бернард Шоу

Симуляция корпоративной сети с ИТ и SCADA сегментами



Security Operations Center

Сервер моделирования компьютерных атак

Готовые шаблоны сетей и сценарии обучения

Ampire развивает навыки:

Проектировать для защиты

Наблюдать и управлять

Собирать и использовать

Расследовать

Использовать и поддерживать

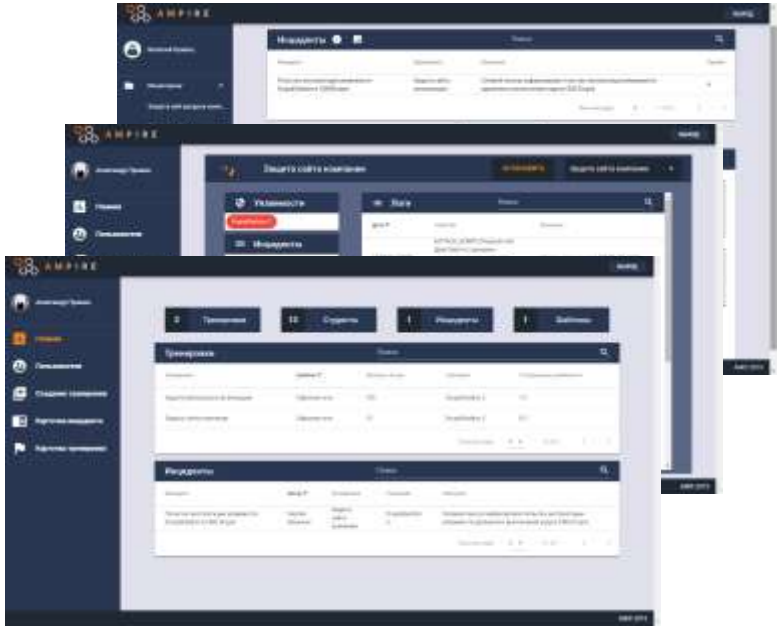
Охранять и защищать

Анализировать

Ролевая модель в Ampire

Киберучения. Примеры сценариев.

- Защита контроллера домена предприятия
- Защита критических рабочих станций предприятия
- Защита финансовых данных предприятия
- Защита данных сегмента АСУ ТП
- Защита научно-технической информации предприятия
- Защита баз данных предприятия



Примеры Киберучений

Варианты применения/функционал

Функции	Варианты применения									
	Тестирование ИБ	Исследование ИБ	Формирование компетенций ИБ	**Обучение ИБ**	Развитие киберзможностей	**Повышение киберустойчивости**	Оценка компетентности	Набор персонала	Цифровая адаптивность	Соревнования ИБ
Координация работы компонент			✓	✓	✓	✓	✓	✓	✓	✓
Симуляция Интернет-сервисов						✓				
Симуляция атак	✓	✓	✓	✓	✓	✓	✓			✓
Симуляция пользователей сети		✓			✓	✓				
Управление компетенциями			✓	✓	✓	✓	✓	✓		✓
Создание сценариев			✓	✓	✓	✓	✓	✓		✓
Сбор и анализ данных		✓	✓	✓	✓	✓		✓		✓
Оценка и отчетность			✓	✓	✓	✓	✓	✓		✓
Инструменты Инструктора			✓	✓	✓	✓	✓			

Киберполигоны для телеком-компаний

«Невозможно управлять направлением ветра, но всегда можно так поставить паруса, чтобы достичь своей цели»
Оскар Уайльд

- Обеспечение компетентности и повышение квалификации собственного персонала по кибербезопасности.
- Поддержка испытательного стенда «цифрового двойника» собственной инфраструктуры для контроля ее кибер-устойчивости.
- Продажа сервисов по проведению семинаров, учебных курсов и сертификационных тестов для промышленных предприятий, банков, малого и среднего бизнеса, колледжей и университетов.

infotecs

Спасибо!