ПЕРВЫЙ ИБ-ШНЫЙ ЖУРНАЛ В КАЗАХСТАНЕ

MSSP

ВЫПУСК №2

ДЕКАБРЬ 2025

ФИШИНГ

репортаж

ОДИН ДЕНЬ С SOC-АНАЛИТИКОМ

(стр. 5)

НЕОБЫЧНЫЙ СПОСОБ ЗАЩИТИТЬ СВОЮ КОМПАНИЮ

(стр. 9)

ОСТОРОЖНО С ПИСЬМАМИ И СООБЩЕНИЯМИ

Памятка для вашей бабушки

(стр. 17)

2025 ГОД:

Опасные уязвимости, бизнес и новости в мире ИБ (стр. 11)

CONT

ENTS

ДОРОГИЕ КОЛЛЕГИ!

Вот и подходит к концу ещё один насыщенный год. Год, в котором мы не просто достигали целей – мы меняли правила игры, открывали новые направления, внедряли технологии, создавали решения, которыми по праву можем гордиться.

За этим успехом стоит команда, объединённая общими ценностями: профессионализмом, взаимным доверием и стремлением быть лучшими.

2026 год станет для нас временем новых горизонтов. Мы будем усиливать наши продукты, укреплять партнёрства и расширять международное присутствие. Но главное – мы продолжим развивать ту культуру, в которой каждый чувствует себя частью чего-то большего.

Пусть Новый год принесёт вам вдохновение, энергию и внутреннюю уверенность.
Пусть каждый день будет шагом вперёд к новым идеям, проектам и личным победам.

С наступающим Новым годом!

Салипов Даурен

CEO MSSP.GLOBAL

2025 ГОД В MSSP ЭТО:

>150 КОНТРАКТОВ, А ТАКЖЕ...

1. **Курсы по кибергигиене для населения теперь доступны в eGov Mobile**
   Каждый урок – это практические советы и простые шаги, которые помогут защитить ваши данные и чувствовать себя увереннее в онлайн-пространстве

2. **Запустили корпоративные курсы на платформе CitizenSec.kz**
   Теперь компании могут системно обучать своих сотрудников кибергигиене: практика, сертификация, измеримый прогресс

3. **Опубликовали 7 экспертных статей на сайте интернет-издания ER10**

4. **Специалист MSSP.GLOBAL Алмас Зейнулин**
   Признан одним из лучших багхантеров Казахстана

5. **Пополнили профессиональную копилку сертификатов**
   HTB CWEE (единственный в Казахстане), OSCP и CRTP

6. **SaaS-решение DODGER вошёл в ТОП-10 стартапов IT Queen 2025**
   Среди более 300 заявок и 90 проектов

7. **Около 90 000 человек прошли обучение по кибергигиене на портале CitizenSec.kz,**
   из них около 10 000 – госслужащие РК

8. **Выступили с докладами и провели воркшоп на международной конференции ICCSDF AI,**
   посвящённой кибербезопасности и искусственному интеллекту

9. **Усилили имиджевые продукты MSSP.GLOBAL**
   Провели масштабную съёмку видеоролика о компании, обновили и презентовали сайт mssp.global, оформили стену проекта CitizenSec на 10 этаже и сделали много-много презентационных материалов

10. **Стали участниками фестиваля Comicon Astana**
    Команда CitizenSec провела интерактив по кибергигиене, а наши партнеры сеть хот-дожных ОМ дарили всем участникам френч-дог

11. **Запустили масштабную информационную кампанию по кибергигиене**
    Баннеры и LED-экраны на городских улицах, соцролик на телеканалах, административных зданиях и СМИ, а также размещение материалов на сайтах госорганов и в соцсетях.

12. **Провели 2 корпоративных обучения по DLP «КиберСтраж»**
    Передали практические знания, разобрали кейсы и показали подходы к защите данных

РЕПОРТАЖ

ОДИН ДЕНЬ С SOC-АНАЛИТИКОМ

Когда за окном ещё темно, а город только просыпается, здесь уже кипит работа. Мониторы светятся графиками, цифрами и уведомлениями. SOC (Security Operation Center) – место, где дежурство не останавливается ни на минуту.

Каждую секунду в центр поступает информация о сотнях событий: подозрительные попытки аутентификации, аномалии в сетевом трафике, попытки взлома. Аналитики SOC первыми встречают угрозы и реагируют до того, как они смогут повлиять на инфраструктуру.

К вечеру одна смена передаёт пост другой. Город засыпает, но SOC не спит никогда, потому что угрозы не знают времени суток.

24/7

Security Operation Center – это центр мониторинга информационной безопасности, который работает непрерывно. Его основная задача предотвращать киберугрозы, защищать инфраструктуру компании и обеспечивать стабильность бизнес-процессов.

Для эффективности работа SOC разделена на уровни ответственности.

Каждый инцидент, как отдельная история: его нужно заметить, проанализировать, подтвердить или опровергнуть, классифицировать и передать дальше.

Любая ошибка может стоить дорого, поэтому каждое действие здесь отточено.

L1 SOC: КРУГЛОСУТОЧНЫЙ МОНИТОРИНГ

Команда первого уровня – это глаза и уши SOC. Они первыми встречают события, которые поступают в систему мониторинга, и принимают решение, есть ли в них признаки угрозы.

Основные задачи L1:

- **24/7 наблюдение в системах SIEM** и других средствах безопасности
- **первичный анализ срабатываний**
- **передача случаев,** требующих углублённого расследования специалистам L2
- **выявление подозрительной активности**
- **классификация событий и регистрация инцидентов**

L1

– это линия, которая держит первый удар. Здесь важны внимание к деталям, скорость реакции и стрессоустойчивость.

L2 SOC: РЕАГИРОВАНИЕ И ГЛУБОКАЯ АНАЛИТИКА

Если инцидент подтверждён, в работу включается второй уровень – команда, которая углубляется в суть угрозы:

- **реагирует** на подтверждённые инциденты
- **проводит** расследование причин и сценариев атаки
- **осуществляет** инженерную поддержку систем безопасности
- **занимается** разработкой и улучшением правил корреляции, playbook'ов и процессов
- **занимается** настройкой и оптимизацией средств мониторинга

L2

– это команда экспертов, которая глубоко разбирает подтверждённые инциденты, усиливает защиту и повышает эффективность реагирования.

ПОЧЕМУ SOC ВАЖЕН ДЛЯ КОМПАНИИ

В условиях, когда количество кибератак растёт каждый год, SOC – это щит, который работает круглосуточно; команда, которая предотвращает возможные сбои в работе компании; система, обеспечивающая прозрачность, контроль и устойчивость в цифровой среде.

Именно здесь ежедневная и почти невидимая работа превращается в надёжную опору всей цифровой инфраструктуры наших партнеров.

ОПАСНЫЕ УЯЗВИМОСТИ 2025 ГОДА:

ЧТО УГРОЖАЕТ ВАШИМ ДАННЫМ И КАК ЗАЩИТИТЬСЯ

САКЕН ТЛЕУБЕРДИН

Руководитель проекта Redteam

В 2025 году количество критических уязвимостей продолжает расти – только во втором квартале эксперты зафиксировали рекордное число новых CVE-идентификаторов. При этом злоумышленники стали активнее использовать уязвимости нулевого дня: Google Project Zero сообщает о 75 таких атаках за 2024 год, причем 44% из них были направлены на корпоративные платформы.

Это означает, что современные угрозы становятся не только сложнее, но и опаснее для обычных пользователей и бизнеса. **Исследователь кибербезопасности, руководитель проекта Dodger компании MSSP.GLOBAL Сакен Тлеубердин поделился самыми опасными уязвимостями 2025 года.**

1 КРИТИЧЕСКИЕ ДЫРЫ В СИСТЕМАХ БЕЗОПАСНОСТИ

CVE-2025-33073 в Kerberos Active Directory стала одной из самых серьезных угроз года. Эта уязвимость позволяет злоумышленникам проводить отраженные атаки через манипулирование DNS-записями и извлекать базу данных Security Account Manager (SAM). Особенно опасно то, что для атаки достаточно отключения подписи SMB или установки значения «при согласовании» – настроек, которые встречаются во многих корпоративных сетях.

CVE-2025-53786 в Microsoft Exchange угрожает тысячам серверов по всему миру. Уязвимость позволяет администраторам локальной версии проникать в облачную среду Microsoft, подделывая токены и API-запросы. По данным Shadowserver, на 10 августа 2025 года обновления не установлены на более 29 тысячах серверов по всему миру.

2 АТАКИ НА ПРОЦЕССОРЫ НОВОГО ПОКОЛЕНИЯ

В 2025 году выявлены новые спекулятивные атаки GhostRace и RFDS, затрагивающие архитектуры Intel, AMD и ARM. Эти уязвимости позволяют извлекать конфиденциальные данные из памяти, включая пароли, ключи шифрования и личную информацию.

3 АТАКИ НА ML-МОДЕЛИ

Развитие ИИ-технологий создает новые векторы атак. Основные угрозы включают:

- Атаки отравления данных: внедрение вредоносных данных в обучающие наборы
- Атаки инверсии модели: восстановление конфиденциальных данных из ответов ИИ
- Атаки уклонения: обман классификаторов через специально подготовленные входные данные
- Кража моделей: извлечение интеллектуальной собственности компаний

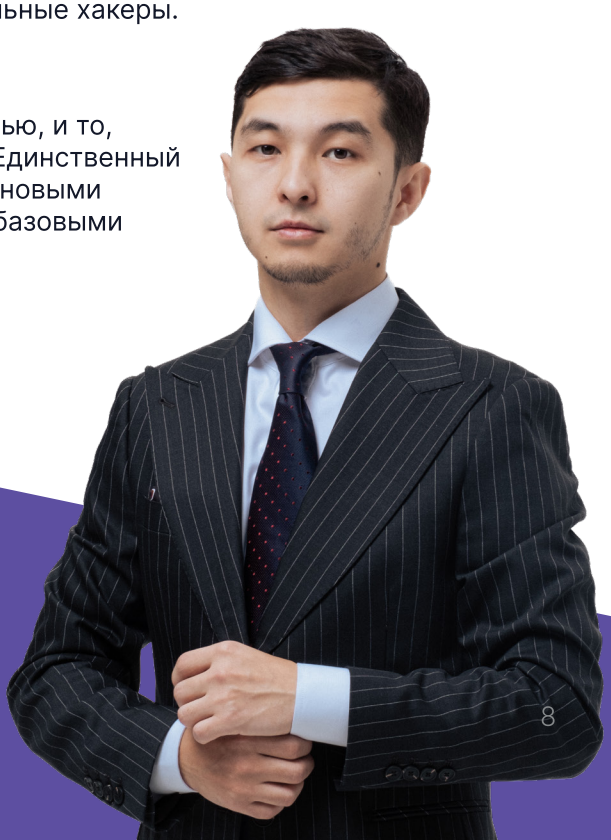
Как распознать уязвимые системы

- Необычная сетевая активность – подключения к неизвестным серверам
- Замедление работы системы без видимых причин
- Появление новых процессов или служб в системе
- Изменения в конфигурации безопасности без ведома администраторов
- Необычные записи в журналах событий

Защита для бизнеса

1. Регулярно обновляйте программное обеспечение – это самая важная мера защиты от известных уязвимостей. Установите автоматические обновления для операционной системы, браузеров и антивирусных программ.
2. Используйте поведенческие системы защиты – современные антивирусы с технологиями EDR (Endpoint Detection and Response) способны обнаруживать даже неизвестные угрозы по их поведению.
3. Внедрите управление уязвимостями – создайте процесс регулярного сканирования и приоритизации исправлений. ИИ поможет определить, какие уязвимости представляют наибольший риск для вашей инфраструктуры. Например, платформа Dodger.kz помогает выявлять уязвимости и работает автономно для сканирования внешней сети и проверяет на утечки данных в Даркнете.
4. Проводите регулярные оценки защищенности вашей организации. Пентест (тестирование на проникновение) – это имитация настоящей кибератаки на вашу компанию. В 2025 году каждая вторая компания сталкивается с кибератаками, но только 12% из них готовы адекватно отреагировать. Пентест дает возможность обнаружить слабые места в вашей защите до того, как их найдут реальные хакеры.

Мир кибербезопасности развивается с невероятной скоростью, и то, что было безопасно вчера, может стать уязвимым сегодня. Единственный способ оставаться защищенным – это постоянно следить за новыми угрозами, регулярно обновлять системы и не пренебрегать базовыми мерами безопасности.



ПОМНИТЕ:

в кибербезопасности не бывает «достаточно безопасно», есть только «безопасно на данный момент».

ФИШИНГ — НЕОБЫЧНЫЙ СПОСОБ ЗАЩИТИТЬ СВОЮ КОМПАНИЮ

Когда мы слышим слово «фишинг», первое, что приходит на ум – опасность. Мошенники, поддельные письма, ссылки, которые ведут прямо в руки злоумышленников.

И это верно. Фишинг остаётся самым распространённым способом кибератак в мире. По данным IBM Security, более 90 % всех инцидентов начинаются именно с письма, которое кто-то открыл, не задумываясь.

Но что, если мы скажем, что фишинг может... защитить вашу компанию?

ФИШИНГ КАК ВАКЦИНА ОТ ФИШИНГА

Как и вакцина, имитация атаки может стать самым эффективным способом выработать «иммунитет». Именно на этом принципе строятся фишинг-тесты – безопасные симуляции реальных атак, которые проводят службы кибербезопасности.

Сотрудникам приходит письмо, очень похожее на обычное: от «службы поддержки», «банка», «коллеги из HR». Если человек переходит по ссылке или вводит данные, система фиксирует реакцию, но не наносит вреда. После теста участники получают короткое обучение – разбирают, что выдало подделку и как отличить фишинг в будущем.

Результат мгновенный и мощный:

- сотрудники начинают внимательнее относиться к письмам;
- снижается число реальных инцидентов;
- формируется привычка «думать перед кликом».

ПОЧЕМУ ЭТО РАБОТАЕТ

Потому что теория не учит внимательности. Можно десятки раз читать памятку «не переходите по подозрительным ссылкам», но мозг не запомнит это, пока не окажется в ситуации.

Фишинг-симуляция создаёт безопасный стресс: человек попадает в «атаку», но выходит без потерь, с новым опытом. В компаниях, где проводят такие тесты раз в квартал, вероятность реального инцидента падает в среднем на 70%.

КАК ПРОВОДИТЬ ФИШИНГ-ТЕСТЫ ГРАМОТНО

Регулярность. Раз в 2–3 месяца оптимально. Часто, но не навязчиво.

Разнообразие. Используйте разные сценарии: корпоративные письма, приглашения на вебинары, рассылки от «банков» или «служб доставки».

Обратная связь. После теста не наказывайте – обучайте. Это инструмент развития, а не контроля.

Аналитика. Считайте метрики: кто открыл, кто кликнул, кто сообщил в ИБ-отдел.

ФИШИНГ С ЧЕЛОВЕЧЕСКИМ ЛИЦОМ

Важно помнить: цель таких симуляций не поймать, а научить. Настоящая сила компании в осведомлённых людях, а не в страхе перед проверкой. Когда сотрудники сами сообщают о подозрительных письмах, а не ждут указаний сверху, тогда организация действительно защищена.

ФИШИНГ — НЕ ВРАГ, А ИНСТРУМЕНТ

Да, фишинг остаётся угрозой № 1. Но, как и в медицине, лучший способ победить вирус – выработать иммунитет. И иногда провести прививку.

Безопасность начинается с осознанности. И если хотя бы одно фейковое письмо поможет предотвратить реальную атаку, значит тест сработал.

КИБЕРБЕЗОПАСНОСТЬ СЕГОДНЯ:

ОБЗОР МИРОВЫХ НОВОСТЕЙ

Мир стремительно цифровизируется, вместе с этим растут и киберугрозы. В 2025 году безопасность перестала быть просто IT-задачей: теперь это стратегический вопрос для каждого бизнеса, от банков до стартапов.

Мы собрали самые актуальные новости из мира ИБ и кратко рассказали, что они значат для компаний, работающих в этой сфере.

ЛЮДИ ВСЁ ЕЩЁ ГЛАВНАЯ УЯЗВИМОСТЬ

Исследование Bitdefender, проведённое среди более чем 7 000 пользователей по всему миру, показало: осведомлённость растёт, но поведение остаётся рискованным. Многие по-прежнему используют простые пароли, игнорируют двухфакторную аутентификацию и легко попадаются на фишинговые письма.

Кроме того, пользователи выражают всё большую тревогу по поводу искусственного интеллекта: с одной стороны, он помогает защищать, с другой – становится инструментом злоумышленников.

Почему это важно:

Компании должны делать ставку не только на технологии, но и на обучение. Курсы кибергигиены, внутренние тренинги и регулярные тесты на осведомлённость сотрудников становятся не роскошью, а обязательной частью культуры безопасности.

ОПАСНЫЕ СЕТИ: ПРЕДУПРЕЖДЕНИЕОТ GOOGLE

Google опубликовал предупреждение: использование публичного Wi-Fi остаётся одной из главных угроз для пользователей. Киберпреступники создают клоны точек доступа или перехватывают данные, что особенно опасно для людей, работающих удалённо.

Почему это важно:

В эпоху гибридных рабочих моделей компании должны пересмотреть политику безопасности: внедрить VPN, шифрование трафика, а также напомнить сотрудникам простое правило – «бесплатный Wi-Fi может стоить дорого».

ВЕЛИКОБРИТАНИЯ УСИЛИВАЕТ ЗАЩИТУ КРИТИЧЕСКИХ СИСТЕМ

Правительство Великобритании представило проект закона, направленный на защиту общественных служб от кибератак. Он обяжет IT-подрядчиков и поставщиков облачных сервисов соблюдать новые стандарты безопасности и уведомлять о любых инцидентах. Кроме того, власти обсуждают запрет на выплату выкупа в случаях ransomware-атак.

Почему это важно:

Регулирование в сфере кибербезопасности становится нормой – не только в ЕС или США, но и в Азии, на Ближнем Востоке, в Казахстане. Для бизнеса это сигнал: важно не просто защищаться, но и соответствовать стандартам. Услуги аудита, консалтинга и внедрения политик безопасности будут расти в спросе.

ВОЛНА АТАК НА ОБЛАКО И IOT

Национальный центр кибербезопасности Великобритании (NCSC) сообщает: количество атак на центры обработки данных и облачные сервисы выросло на 50 %.

Злоумышленники всё чаще нацеливаются на слабозащищённые IoT-устройства и сетевые сервисы, через которые получают доступ к корпоративной инфраструктуре.

Почему это важно:

Границы безопасности размылись. Современные решения должны охватывать не только серверы и офисные сети, но и облачные сервисы, удалённые устройства, мобильные рабочие станции.

АТАКИ ЧЕРЕЗ ЦЕПОЧКУ ПОСТАВОК НАБИРАЮТ ОБОРОТЫ

Исследования показывают, что угрозы, связанные с цепочками поставок (third-party & nth-party), становятся одной из самых серьёзных точек входа для злоумышленников. По данным отчёта ReversingLabs «Software Supply Chain Security 2025», атак такого типа становится больше, они охватывают открытые и закрытые программные решения и связаны как с ИИ-моделями, так и с коммерческим ПО.

Почему это важно:

Для ваших клиентов, особенно с распределёнными поставщиками и партнёрами, это значит, что защита должна быть не только внутри компании, но и во всех звеньях цепочки. Аудит поставщиков, мониторинг связей, сегментация доступа и контроль обновлений — становятся критичными элементами программы информационной безопасности.

2025 ГОД ПОКАЗЫВАЕТ: КИБЕРБЕЗОПАСНОСТЬ ПЕРЕСТАЛА БЫТЬ «ДЕЛОМ IT».

Это комплексная экосистема, где важны технологии, люди и культура. Пока кто-то считает безопасность затратами, другие уже превращают её в конкурентное преимущество и именно эти компании войдут в 2026 год с уверенностью и устойчивостью.

ОКНО В ДАРКНЕТ:

КАК УЗНАТЬ, ЧТО ПИШУТ О ТЕБЕ В ДАРКНЕТАХ ПО ЦЕНЕ ЧАШКИ КОФЕ

Цифровая среда стремительно усложняется, но парадокс заключается в другом: большинство успешных кибератак происходят не из-за гениальности хакеров. Сегодня до 80% инцидентов связаны с обычными человеческими ошибками – забытым тестовым сервисом, неустановленным обновлением, случайно открытым портом или паролем, который давно всплыл в даркнете.

Пока компании обсуждают «сложные таргетированные атаки», автоматические сканеры злоумышленников каждую секунду проходят по интернету, высвечивая уязвимости быстрее, чем их замечает внутренняя команда. Если ошибка найдена, то последствия наступают мгновенно: данные шифруются, уничтожаются или просто продаются на теневых площадках.

Возникает главный вопрос современной кибербезопасности: знаете ли вы, что злоумышленники уже сейчас видят о вашей инфраструктуре?

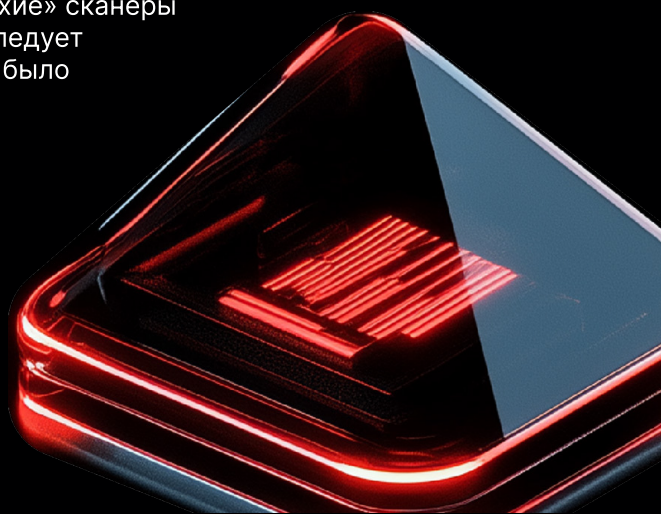
Возникает главный вопрос современной кибербезопасности: знаете ли вы, что злоумышленники уже сейчас видят о вашей инфраструктуре?

КОГДА УГРОЗЫ ПРИХОДЯТ САМИ: РЕАЛЬНОСТЬ STATUS QUO

Интернет – это бесконечный поток сканирования. Два типа ботов смотрят на вашу инфраструктуру тысячу раз в день:

- **«Хорошие»** – поисковики Google и Yandex
- **«Плохие»** – автоматические сканеры, созданные для поиска уязвимостей

В отличие от поисковиков, которые индексируют сайты, «плохие» сканеры охотятся за ошибками и мгновенно используют их. Отсюда следует простой, но болезненный вывод: большинство утечек можно было предотвратить, если бы риски были замечены вовремя.



DODGER

Cybersecurity без границ

ПОСМОТРИТЕ НА СВОЮ КОМПАНИЮ ГЛАЗАМИ ТЕХ, КТО ИЩЕТ СЛАБЫЕ МЕСТА

DODGER – SaaS-решение MSSP.GLOBAL, которое даёт руководителям компаний беспрецедентную прозрачность. Это инструмент, который показывает:

- что доступно в интернете о вашей инфраструктуре;
- какие сервисы открыты, пусть даже забыты давно;
- какие критичные уязвимости могут быть использованы превентивно;
- какие пароли сотрудников уже появились в даркнете.

DODGER

создаёт честную картину, которую обычно видят хакеры. Но теперь первым видите её вы.

Как это работает?

1. DODGER сканирует вашу публичную инфраструктуру за считанные минуты
2. Находит все активные сервисы, включая скрытые и тестовые
3. Выявляет уязвимости с приоритизацией. Показывает утечки паролей
4. Предоставляет чёткий план действий по устранению найденных рисков

То, что раньше требовало недели ручной работы, теперь доступно быстрее, чем успевает остыть утренний кофе.

Подобное сканирование необходимо всем организациям с публичной инфраструктурой: от банков и государственных структур до корпораций, IT- и телеком-компаний.

Ведь если у вас есть публичный ресурс – у вас есть поверхность атаки.

А ЗНАЧИТ, ВАМ НУЖЕН DODGER.

7 ФИЛЬМОВ О МИРЕ IT И КИБЕРБЕЗОПАСНОСТИ

Каждый из фильмов по-своему рассказывает о цене прогресса. О том, что технологии не бывают нейтральными. Они несут ответственность, формируют новые системы власти и этические дилеммы.

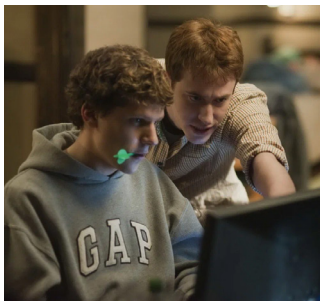
WHO AM I: KEIN SYSTEM IST SICHER (2014)

Жанр: триллер, драма

Бенджамин – молодой компьютерный гений. С детства он мечтает стать супергероем из комиксов и покорить мир. Но в реальном мире он – никто. Его жизнь неожиданно меняется, когда он встречает свою полную противоположность – харизматичного Макса. Не желая жить в жёстких рамках системы, они совершают череду дерзких кибер-преступлений. Восстав против равнодушного общества, они становятся кумирами для целого поколения. Теперь Бенджамин не просто супергерой, он – самый разыскиваемый хакер в мире.

Почему смотреть:

Фильм мастерски соединяет напряжение триллера и визуальную эстетику киберпанка. В нём показано, как тонка грань между игрой в хакера и настоящим преступлением. Главная идея – поиск идентичности и признания в цифровом мире, где анонимность соблазнительна, но иллюзорна.



THE SOCIAL NETWORK (2010)

Жанр: биографическая драма

Осенью 2003 года студент Гарварда Марк Цукерберг, движимый амбициями и личными обидами, создаёт сайт, который навсегда изменит представление о коммуникации в сети. Сначала это студенческое развлечение, затем – стартап, а вскоре – глобальная платформа, где миллионы людей делятся своими жизнями. Фильм показывает не просто рождение Facebook, а эволюцию идеи: от ночной строчки кода до империи данных и судебных исков.

Почему смотреть:

В центре сюжета конфликт между гениальностью и моралью, скоростью и этикой, деньгами и смыслом. Отличная иллюстрация того, как одна идея способна изменить цифровую экосистему и общество.

MR. ROBOT (2015–2019)

Жанр: сериал, психологический триллер

О чём: Эллиот Алдерсон – талантливый, но глубоко одинокий инженер по кибербезопасности, который днём защищает компании от взломов, а ночью сам становится хакером-мстителем. Однажды Эллиот встречает загадочного анархиста, известного как Мистер Робот, и присоединяется к подпольной группе fsociety, мечтающей уничтожить мировой финансовый порядок, стерев долги и зависимость людей от корпораций. Но чем глубже он погружается в борьбу, тем больше теряет контроль над собой и над тем, где проходит грань между реальностью и иллюзией.

Почему смотреть:

Самая достоверная визуализация хакерской культуры и атак. Однако в центре не технологии, а психология человека в цифровую эпоху: одиночество, чувство бессмысленности и попытка вернуть контроль над жизнью в мире, где всё – данные.

SNOWDEN (2016)

Жанр: биопик, триллер

Фильм основан на реальных событиях, изменивших представление человечества о конфиденциальности и свободе в цифровую эпоху. Эдвард Сноуден – талантливый аналитик и сотрудник Агентства национальной безопасности США (АНБ). Его карьера развивается стремительно: он проектирует системы наблюдения, работает под грифом «совершенно секретно» и уверен, что служит своей стране.

Но чем глубже он погружается в операции АНБ, тем яснее осознаёт: слежка ведётся не только за террористами, но и за обычными гражданами по всему миру. Правительства используют технологии не для защиты, а для контроля.

Понимая, что молчание делает его соучастником, Сноуден решается на невозможное: похищает секретные документы и передаёт их журналистам, раскрывая миру масштаб глобальной слежки.

Почему смотреть:

Фильм не героизирует Сноудена, но показывает его внутреннюю эволюцию: от солдата цифрового фронта до человека, который ставит совесть выше карьеры, репутации и свободы.

ZERO DAYS (2016)

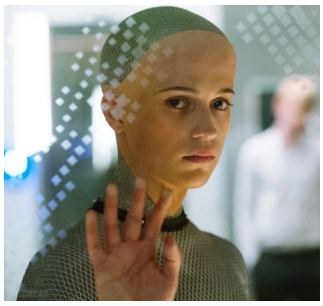
Жанр: документальный

Документальный фильм, который рассказывает о самой громкой кибератаке в истории – появлении вируса Stuxnet, созданного для поражения иранских ядерных объектов. Это первое в мире кибероружие, способное физически вывести из строя промышленное оборудование.

Расследуя происхождение вируса, журналисты и эксперты постепенно приходят к выводу, что за его созданием стоит совместная операция спецслужб США и Израиля под кодовым названием Olympic Games. Но история выходит за рамки одной атаки: фильм показывает, как гонка кибервооружений стала новой формой холодной войны, где вместо ракет – строчки кода, а поле боя – инфраструктура всего мира.

Почему смотреть:

Понимание реальных масштабов кибервойн. То, что раньше казалось фантастикой, давно стало частью геополитики.



EX MACHINA (2014)

Жанр: фантастика, философский триллер

Калеб – молодой программист из IT-компании, выигравший внутренний конкурс на участие в секретном проекте. Он отправляется в изолированный высокотехнологичный дом-лабораторию в горах, где его ждёт харизматичный и пугающий гений Натан. Тот поручает Калебу провести модифицированный тест Тьюринга – определить, обладает ли искусственный интеллект по имени Ава настоящим сознанием.

Но чем больше Калеб общается с Авой, тем сильнее ощущает, что она не просто программа. Её взгляд, эмоции и попытки сбежать из плена заставляют его усомниться: кто здесь человек, а кто объект эксперимента? Вскоре становится ясно, что наблюдатель сам стал частью эксперимента и возможно, вовсе не в роли, на которую рассчитывал.

Почему смотреть:

Минималистичный, но глубокий фильм о границах сознания и этике создателей технологий. Заставляет задуматься, кто на самом деле проходит тест Тьюринга – машина или человек.

THE BILLION DOLLAR CODE (2021)

Жанр: мини-сериал, драма

Берлин, 1990-е годы. Молодой художник-цифровик Карстен и программист-инженер Юри создают в подпольной студии проект под названием TerraVision – инновационное приложение, позволяющее «летать» над Землёй в трёхмерной визуализации спутниковых снимков.

Проходит десять лет. Парни узнают, что компания Google выпустила Google Earth – продукт, удивительно похожий на их TerraVision. Начинается юридическая и моральная борьба Давида против цифрового Голиафа: два немецких идеалиста против транснациональной корпорации, у которой безграничные ресурсы, но нет души их изобретения.

Почему смотреть:

Драматичная история о креативности, справедливости и борьбе независимых разработчиков против гигантов индустрии.

ПАМЯТКА ДЛЯ БАБУШКИ:

НАВЕСТИ ЕЁ И РАССКАЖИ О КИБЕРГИГИЕНЕ

Бабушки – самые заботливые люди. Они беспокоятся о нас, звонят, чтобы спросить, ели ли мы, и всегда хотят помочь. А теперь настало время нам позаботиться о них. Потому что интернет сегодня не только удобство, но и место, где легко попасться на уловки мошенников.

1 НЕ СПЕШИ ОТВЕЧАТЬ НА ЗВОНКИ И СООБЩЕНИЯ ОТ «СЛУЖБ БЕЗОПАСНОСТИ»

Если звонят и говорят, что с карты что-то случилось – не паникуй. **Никогда не называй код из SMS, логин или пароль.** Настоящий банк не будет спрашивать такие данные. Лучше положить трубку и сама перезвони в свой банк по официальному номеру.

2 ОСТОРОЖНО С ПИСЬМАМИ И СООБЩЕНИЯМИ

Мошенники часто присылают «важные уведомления» будто бы от госуслуг, банка или оператора. Если письмо просит срочно перейти по ссылке, ввести пароль или скачать документ **– удали его.**

Можно просто позвонить внукам или детям и уточнить, правда ли это.

3 НЕ УСТАНАВЛИВАЙ ПРОГРАММЫ И ПРИЛОЖЕНИЯ ПО ПРОСЬБЕ НЕЗНАКОМЦЕВ

Никаких «удалённых доступов», «программ для связи с банком» и «новых антивирусов». Если кто-то просит установить, разрешить доступ или ввести код **– это почти всегда мошенники.**

4 ДЕРЖИ ТЕЛЕФОН И ПАРОЛЬ ПРИ СЕБЕ

Не называй PIN-коды даже близким по телефону. Храни пароли в записной книжке дома, а не в заметках телефона. Если кто-то попросит «дать телефон на минутку» – не соглашайся.

5 ОСТОРОЖНО С ПОКУПКАМИ В ИНТЕРНЕТЕ

Сайтов сейчас много, и не все честные. Покупай только там, где сайт начинается с https:// и есть отзывы. Если цена слишком низкая – скорее всего, это обман.

6 И ГЛАВНОЕ – НЕ СТЕСНЯЙСЯ СПРАШИВАТЬ

Если что-то непонятно – позвони детям или внукам. Лучше спросить, чем потом переживать. Интернет может быть безопасным местом, если пользоваться им с вниманием и спокойствием.

КАК ПРОШЛИ DEMO-DAY В MSSP.GLOBAL

В 2025 году мы провели не один, а сразу два Demo-day, где команды показали друг другу, как именно рождаются продукты, решения и улучшения, которыми мы гордимся. Это внутреннее окно в процессы, благодаря которому мы лучше понимаем:

- чем живут разные проекты
- какие результаты достигаются прямо сейчас
- куда движется вся компания в целом

Живые демонстрации, честные выводы и открытые разговоры – всё это позволяет по-новому взглянуть на нашу работу и ощутить реальную синергию.

В июне и сентябре мы поделились не только цифрами и метриками, но и реальными практиками: что сработало лучше всего, какие гипотезы не подтвердились, чему научились и что планируем внедрять дальше.

ПОЧЕМУ ВАЖНО ПРИХОДИТЬ НА DEMO-DAY

Потому что это возможность:

- увидеть картину компании целиком
- познакомиться с ключевыми достижениями квартала
- услышать о планах и вызовах проектов
- задать вопросы и повлиять на развитие
- почувствовать общую динамику MSSP.GLOBAL

Такие встречи напоминают нам о простом, но важном принципе: когда мы делимся опытом открыто, мы растём не только как отдельные проекты, но и как единая команда.

КАЖДЫЙ РАЗ НА СЦЕНУ ВЫХОДИЛИ ПО ТРИ КОМАНДЫ MSSP.GLOBAL:

CitizenSec

Показали развитие обучающей платформы, новые инструменты для пользователей и обновлённый корпоративный кабинет.

SOC

Команда рассказала о работе 24/7, внедрении автоматизаций, сценариях реагирования и улучшениях в процессе мониторинга.

Red Team

Команда поделились свежими кейсами проверок, инсайтами по безопасности и тем, какие векторы атак становятся наиболее актуальными.

Кроме того, обсуждали важные темы: как эффективно работать с отделом маркетинга, как функционирует система DLP, а также какие варианты развития ждут

КИБЕР-ГОРОСКОП НА 2026 ГОД

2026-й обещает быть насыщенным на апдейты, фишинговые ловушки и киберсюрпризы. Главное – не кликайте по сомнительным ссылкам судьбы и держите антивирус интуиции включённым.

♈ ОВЕН

В этом году ты снова на передовой. Лезешь в бой с угрозами, не дожидаясь патча. Но, пожалуйста, делай бэкап перед каждым решением.

Совет: иногда «Alt+F4» – это тоже стратегия.

♉ ТЕЛЕЦ

Ты стабильный, надёжный и всегда на дежурстве. Но не всё, что кажется безопасным, стоит сохранять в памяти.

Совет: чисти кеш эмоций хотя бы раз в месяц.

♊ БЛИЗНЕЦЫ

Ты умеешь уговорить даже антивирус расслабиться. В 2026-м используешь харизму на максимум – только не на фишинг коллег.

Совет: фильтруй базу контактов – не все друзья надёжные узлы.

♋ РАК

Ты чувствуешь всё, даже когда сервер ещё не завис. Год подарит стабильность и немного драмы (но безопасной).

Совет: не храни чувства в открытом доступе.

♌ ЛЕВ

Тебе нужны аплодисменты, но система требует обновлений. В 2026-м получишь признание – главное не перегореть от славы, как сервер под нагрузкой.

Совет: даже королям нужен тайм-аут на перезагрузку.

♍ ДЕВА

Ты бы обновил всё: от рабочих процессов до судьбы. 2026-й принесёт успех, если перестанешь исправлять чужие баги в личной жизни.

Совет: иногда «ошибка 404» это просто знак отдохнуть.

♎ ВЕСЫ

Ты всегда стараешься быть добрым и вежливым, даже с фишингом. В 2026-м звёзды советуют: меньше «разрешить доступ всем», больше «только по запросу».

Совет: личные границы – лучший антивирус от хаоса.

♏ СКОРПИОН

В 2026-м ты вскроешь чужие тайны, но ради добра. Станешь мастером психоанализа и кибербезопасности в одном лице.

Совет: не ломай систему, если можно красиво обойти авторизацию.

♐ СТРЕЛЕЦ

Ты любишь апдейты: и системы, и жизнь. В 2026-м установишь пару больших обновлений – одно для паспорта, другое для души.

Совет: не запускай установку «жизнь v2.0» без бэкапа привычного комфорта.

♑ КОЗЕРОГ

Ты – главный по стратегиям, политике и отчётам для Вселенной. Всё идёт по плану, пока кто-то не спросит «А зачем столько паролей?»

Совет: расслабь контроль и доверься процессу, даже ISO не всё стандартизирует.

♒ ВОДОЛЕЙ

Ты придумываешь то, что остальные ещё боятся гуглить. В 2026-м ты снова удивишь коллег, только сначала протестируй на баги.

Совет: меньше хаоса в креативе, больше 2FA в личной жизни.

♓ РЫБЫ

Ты чувствуешь фишинг за версту, но всё равно кликаешь, «а вдруг не обман?». В 2026-м эмоции станут твоей суперсилой, если не утонешь в логах.

Совет: слушай внутренний фаервол, он знает, что опасно.

ГЛАВНАЯ УГРОЗА 2026 – НЕВНИМАТЕЛЬНОСТЬ

ГЛАВНОЕ ОБНОВЛЕНИЕ – ОСОЗНАННОСТЬ

А ЛУЧШИЙ АНТИВИРУС – ЧУВСТВО ЮМОРА

STAY SECURE. STAY KIND. STAY HUMAN

MSSP GLOBAL

MSSP.GLOBAL – КОМПАНИЯ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

ПРОДУКТЫ:

КИБЕРСТРАЖ

DLP-комплекс «Киберстраж»

Современное решение для предотвращения утечек информации. Обеспечивает непрерывный мониторинг информационных потоков, анализируя их на предмет нарушений политик безопасности

DODGER

SaaS-платформа, которая показывает, какие уязвимости могут заметить хакерские сканеры, а также дает рекомендации по их устранению

citizensec

Образовательный проект, направленный на повышение цифровой грамотности и обучение граждан Казахстана основам информационной безопасности

CLOUDTEK

Защищенное облако для вашей организации

УСЛУГИ:

- Penetration testing
- Подготовка к испытаниям
- Security operation center (ОЦИБ)
- Аудит информационной безопасности
- Red Teaming

MSSP
GLOBAL

+7 700 333 0645
INFO@MSSP.GLOBAL

ХОТИТЕ ЗАЩИТИТЬ СВОИ ДАННЫЕ?

Сканируйте QR-код и узнайте, как наши решения в области кибербезопасности помогут вам и вашему бизнесу

ПОДПИШИТЕСЬ НА НАС В ИНСТАГРАМ

Узнайте больше о жизни нашей компании