ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

№09(69) • СЕНТЯБРЬ • 2004

ХАКЕР

WWW.XAKEP.RU

2 ВИДЕО ПО ВЗЛОМУ!

ВЗЛОМ ПО-ЯПОНСКИ

Нашумевшие истории крупных взломов Стр. 60

Приватный канал

Вся инфа о VPN Стр. 68

Стр. 116

Делаем FreeBSD безопасной

FreeBSD: Top Security

Стр. 66

Маленький гигант большого интерфейса

Грамотная подмена системных бинарников

+ Весь архив видео по взлому на DVD

Стр. 102

Хроники ЦэЦэ

Репортаж с крупнейшей демопати России

Стр. 84

Как ломали Глюкозу.ru

Криворуким отечественным администрам посвящается

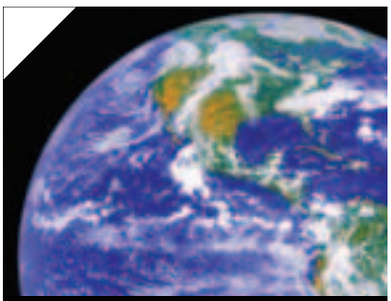
ISSN 1609-1019

(game)land

В ЖУРНАЛЕ

НА DVD БОЛЕЕ 4 ГИГАБАЙТ

- Microsoft Windows XP SP2 (EN)
- Network Security Toolkit 1.0.6
- Delphi 8 for .NET
- Софт на каждый день
- Лучшие демки с Chaos Construction
- Программы от Macromedia
- Музыка
- Софт из журнала
- etc.



INTRO

Вышел на киноэкраны фильм "Послезавтра". Все ринулись смотреть. Много шума наделала кинолента. А ведь не вымысел там, по большейто части. Все эти резкие перемены климата, глобальные потепления и похолодания - все это уже сейчас начинает проявляться. Все лето я сидел без интернета, потому что ежедневно после грозы выгорали хабы, свичи и роутеры. Ну ведь не было раньше такого, чтобы ежедневно гроза :(. Да и взять, к примеру, Сибирь: летом до 40 градусов выше нулевой отметки - диву даться! А в Москве торчим все бледные от недостатка ультрафиолета.

Или вот еще пример: отшумевший совсем недавно фильм "Я, робот" с Уиллом Смитом в главной роли. Кажется, что гонево все это. Совсем недалекое будущее показывают, а там уже какие-то консервные банки видят сны, потому что искусственный интеллект люди для них разработали такой, что от обычного человеческого разума и не отличишь сразу.

Годом раньше, годом позже, но мы придем к этому. Человечество и технический прогресс идут семимильными шагами по тропе развития. Совсем недавно наши отцы сидели на ЕС'ках, а прошло полтора десятка лет, и мы юзаем уже трехгигагерцовые пни. Электронные собачки Айбо уже могут сами вырабатывать фекалии из подручных средств, чем приводят в неописуемый восторг детишек своих хозяев. А роботы, помогающие людям уже практически во всем, хоть и не отличаются пока что особым интеллектом, но становятся день ото дня все умнее и универсальнее.

И вот смотрю я на это все и жалею, что родился так рано. Хотя бы на век позже родиться. Хотя бы одним глазиком взглянуть, что там будет через сто лет! Мы родились так рано. Так много еще хочется увидеть, но, видимо, не судьба :(.

А пока же мы делаем журнал "Хакер". И, как создатели такого прогрессивного журнала, стараемся не только донести самую свежую информацию до читателей, но и даже заглянуть на день вперед, рассказывая о том, о чем еще никто не рассказывал. А ты, дорогой читатель, надеюсь, именно за это нас и любишь.

b00b1ik

CONTENT

SSH НА ПОПАТКАХ

СТР.30

Выбираем SSH-клиент для удаленной работы с сервером.

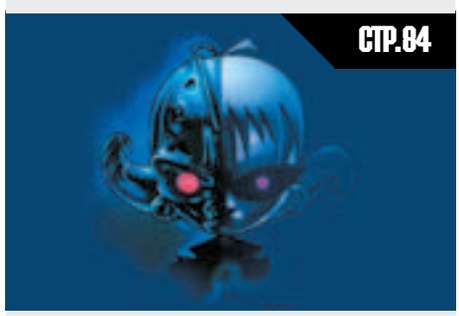
ВООРУЖИСЬ СВОИМ РУТКИТОМ

СТР.64

Прячем свои следы на сервере - устанавливаем правильный руткит.

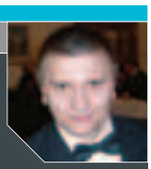
КАК ПОМАЛИ ГЛЮКОЗУ.RU

СТР.84



История о том, как кривоукость админов привела к взлому крупного сайта.

Вячеслав Янсимов aka ansi (ansi@lenta.ru)



БЕЙ ЛАЗЕРОМ ПО БАНКАМ

Стараниями писателей-фантастов и голливудских киношников роль вооружения будущего прочно закрепилась за энергетическим оружием. Это те самые бластеры, лазеры, пучеметы и прочие штуковины, стрепяющие мощными потоками частиц, разрядами, электромагнитными излучениями и другими бестелесными субстанциями. Их главным преимуществом перед пулями и снарядами является мгновенное поражение цели. Идея квантового скачка в новую эру вооружений давно занимает умы военных. В сегодняшнем обзоре читай о самом интересном футуристическом оружии и перспективах модернизации классики.

ВООРУЖЕНИЕ ВЕКА ХАЙ-ТЕК

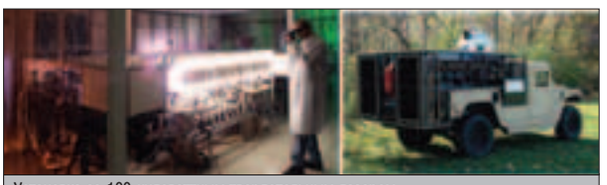
Последние десятилетия кипит работа над прототипами разнообразного энергетического оружия, проводятся его испытания. Законы физики ставят перед современными технологиями такие барьеры, преодоление которых требует нереальных экономических затрат. Пушки стоимостью более 100 миллиардов долларов за штуку не по карману даже Пентагону. Больше всего денег вбухано в космические системы. Однако об их реальном боевом применении говорить пока рано. Ближе всех к практической реализации оказались мощные наземные и корабельные установки средней дальности. Но и они пока воспринимаются как очень и очень дорогие игрушки. Идеи индивидуального энергетического оружия на деле являются далекими и фантастическими.

ЛАЗЕР С ЛАЗЕРНЫМ ПРИЦЕЛОМ

Области применения лазеров необозримы. Куда ни сунься - кругом лазеры. Они используются в медицине, связи, электронике и голографии. Хотя физическая суть у всех лазеров общая, принципы работы, как и возможности, различаются. Военные ценят способность лазеров концентрировать огромную энергию в очень узком луче. Это реально высокоточное оружие. На дальности 10 километров можно получить пятнышко диаметром всего 1 сантиметр. При этом твердотельный лазер мощностью всего 10 киловатт способен создавать луч с плотностью энергии в миллионы раз большей, чем на поверхности Солнца. Промышленные лазеры уже сегодня, как масло, режут стальные и титановые листы. Почему же карманный гиперболоид инженера Гарина до сих пор остается несбыточной мечтой?

В первую очередь, нужна энергия для накачки лазера. Чтобы получить пару десятков киловатт при КПД 20%, придется таскать с собой дизель-генератор весом несколько тонн. Остальные 80% будут расходоваться на тепло, которое необходимо отводить, иначе агрегат просто расплавится вместе со стрелком. Вентиляторами и водичкой тут не обойтись. Кроме того, сами фокусирующие устройства должны иметь приличные размеры для наименьшего расхождения луча на больших дальностях. Установкам необходим еще и точный прицел, желательно лазерный. Шмалять наугад основным лучом - дело бесперспективное.

Футурологи уверенно предсказывают изобретение компактных источников большой энергии. Действительно, в недрах атомных ядер и в химических реакциях скрыта колоссальная энергия, которую нужно лишь аккуратно высвободить. Но пока это удается сделать только в сопровождении взрыва. Правда, есть атомные электростанции, но они еще очень далеки от компактности. Сегодня о боевых лазерах можно говорить лишь как о стационарных вариантах для средств, способных нести многотонные силовые установки, - кораблей, самолетов, космических платформ.



Установка со 100-киловаттным твердотельным лазером

Первые серьезные испытания мощных лазеров класса «земля - воздух» проводились Пентагоном в начале 80-х годов. На поли-

Пульт управления MIRACL. За четверть века проведено более 150 испытаний общей продолжительностью воздействия лазером 3000 секунд

гоне Уайт Сэндс в Нью-Мексико была наглядно продемонстрирована возможность поражать баллистические ракеты. Химический лазер MIRACL мощностью 2 мегаватта с расстояния 1 км дырявил неподвижно закрепленную вторую ступень ракеты Titan-1, раскрашенную под советскую с соответствующей маркировкой. Чтобы сильнее бабахнуло, «Титана» накачали сжатым газом. За 12 секунд «Чудо» так нагрело ракету, что, по словам руководителя программы СОИ, «лазер разнес эту штуковину буквально на куски».

За 20 лет американцы доросли до первого тактического лазера, приспособленного для реального боевого применения. Совместно с израильтянами они совершенствуют мобильную систему MTHEL (проект «Наутилус»). Установка неоднократно была опробована в деле. Она успешно сбивает реактивные снаряды «Хезболла». Близки к завершению и разработки твердотельных лазеров для поражения наземных и воздушных целей. Эти аппараты можно будет перевозить на джипе. Разрабатываются самолетные лазеры большой мощности.

Советский Союз экспериментировал с боевыми лазерами с 70-х годов. В подмосковном Троицке был создан газовый лазер мощностью 1 мегаватт. Установка, аналогичная MIRACL, была построена в Таджикистане. Существовали и другие проекты. В 1987 году ракетой-носителем «Энергия» на орбиту была выведена 80-тонная боевая лазерная станция «Скиф-ДМ» («Полюс»). Но с замораживанием гонки вооружений эксперименты по стрельбе в космосе были отменены. К великой радости американцев, у которых до сих пор нет средств доставки на орбиту таких гигантских конструкций. «Скиф-ДМ» затопили в Тихом океане.

Ракета-носитель «Энергия» с полезной нагрузкой «Скиф-ДМ» («Полюс»)

СПУТНИКИ-ШАХИДЫ

Космические лазеры, поражающие баллистические ракеты противника за тысячи километров, теоретически будут еще больше в размерах. Так, химические лазеры для накачки требуют тонны топлива, охлаждающего вещества и компонентов самого рабочего тела, которое расходуется при каждом выстреле. Фокусирующие зеркала должны быть большими и весьма тяжелыми. Самыми мощными из таких лазеров являются так называемые газодинамические. По сути, это реактивные двигатели, где молекулы фтористого водорода ускоряются до сверхзвуковых скоростей. Такой выхлоп нарушает привычные представления о том, что у лазеров не бывает отдачи. В открытом космосе один выстрел унесет всю платформу вместе с лазером в очень далекое путешествие. Для компенсации реактивного импульса понадобятся дополнительные двигатели и много топлива.

Между прочим, проблема отдачи была решена советскими инженерами еще в 70-х годах. Каким образом - военная тайна ;-). Конструкторы ухитрились установить на пилотируемую станцию «Алмаз» 30-миллиметровую авиационную пушку Нудельмана для отстрела вражеских звездолетов при сближении. Космонавты даже успешно из нее постреляли, сохраняя орбиту и точную ориентацию станции.

Для звездных войн Пентагон готовит рентгеновские лазеры с ядерной накачкой. Они достаточно мощные, но намного компактнее химических. У этих лазеров только один «маленький» недостаток - одноразовость. Мощный импульс излучения рентгеновских лазеров формируется в момент взрыва небольшого термоядерного заряда. Мировое сообщество всеми силами препятствует выводу на орбиту любых ядерных установок. Поэтому запускать такие платформы Пентагон рассчитывает непосредственно при начале ракетной атаки противника. Существует вариант «ронять» спутники на цели с последующим термоядерным взрывом.

ХИРУРГИЯ ГЛАЗА

Вспоминаю свое первое знакомство с лазером, когда еще не было ни сидиромов, ни эксимеров и лазерные указки не продавались в каждом ларьке. На лабораторном занятии я подносил стеклянную призму в красивый рубиновый луч лазера и отклонял его в открытое окно соседнего здания. За что был наказан преподавателем-подполковником, так как вполне мог засветить кому-нибудь в глазик. Мощности тех лазеров хватало лишь на пробивание дырок в копировальной бумаге для последующих замеров штангенциркулем (проверяли расходимость луча). Однако ожог сетчатки при «удачном» попадании был почти гарантирован.

Вряд ли у тебя получится сконструировать самодельный лучемет, разобрав старый сидюк или даже резак, который на раз прожигает болванки. Чтобы полупроводниковый лазер мощностью около 30 милливатт повредил глаз, нужно обеспечить прямое попадание в зрачок. А для этого придется пялиться непосредственно в выходное отверстие лазера. Прицельное наведение в глаза выполнить непросто. Инфракрасный луч невидим, хотя очень опасен. Светить лазером в дверные глазки бесполезно, так как пластиковая оптика для этого диапазона непрозрачна. В случае с приличной оптикой, например, в приборах ночного видения снайперов, в танках и самолетах, ослепить можно по полной программе.

Женевская конвенция запрещает создание и использование ослепляющего оружия, считая его зверским. США ратифицировали соответствующий протокол в 1999 году, и, по идее, должны были снять с вооружения подствольный лазер Sabre 203, прикрепляемый к винтовке M-16. Эта штука пускала красные зайчики с гарантией ослепления на дальности до 300 метров. Запрет имеет оговорки. Так, если в самолет ударил луч боевого лазера с намерением просверлить в нем дырку, но попал при этом в глаз летчику, никаких нарушений усмотрено не будет. Лазейку активно используют. В 2001 году российские ученые создали более мощный и универсальный аналог Sabre 203, позиционируя его как инструмент борьбы с террористами. Кроме подствольного, он существует в самостоятельном варианте с телескопической оптической системой.

ВСЕ ПУЧКОМ

Современные лазеры являются наиболее проработанным видом энергетического оружия. Остальные находятся на стадии идей, теоретических изысканий и экспериментов. Следует выделить пучковое оружие. Его поражающая сила заключена в высокоэнергетических элементарных частицах - электронах, протонах и нейтронах, разгоняемых с помощью линейных ускорителей - синхрофазотронов. Разрушительная мощь таких потоков может быть очень велика, значительно больше, чем у световых квантов. Механизм воздействия отличается от лазерного. В то время как лазер сначала должен пробить поверхность (оболочку) объекта, элементарные частицы проникают вглубь вещества и нарушают работу цели изнутри.

Поток частиц со скоростями, близкими к световой, мгновенно уничтожает цель на расстоянии нескольких километров. Однако эксперименты показали, что частицы неслабо нагревают воздух. Воздух ионизируется, и электрические силы закручивают пучок, который при этом может свернуться в кольцо. Все равно что стрелять из автомата в ванной комнате. Чтобы этого не произошло, можно, например, пробить для пучка канал к цели при помощи мощного лазера.

Синхрофазотрон - вещь серьезная. Помимо наземных вариантов, разместить такую дуру весом в десятки тонн можно разве что на авианосце. Военные моряки намерены использовать боевые ускорите-

◢ Рекомендую книгу Шмыгина А.И. «СОИ глазами русского полковника», 2000 г. Текст можно найти в интернете

◢ Если инопланетяне вдруг презентуют тебе мощный ручной лазер, не стреляй там, где накурено или много пыли. Сгоришь.

◢ Все о рельсовых пушках: www.railgun.org

> «Я марсианин! - сказал он глуховатым голосом. - Всем оставаться на местах, иначе пущу в ход аннигилирующий бластер с фамагустой».
>
> *Георгий Шах. «О, марсиане!»*

ли частиц для поражения противокорабельных крылатых ракет.

ПЛАЗМЕННЫЕ КЛИЗМЫ

Плазма, она же ионизированный газ, - четвертое агрегатное состояние вещества, самое распространенное во Вселенной. Агрегаты, способные вырабатывать высокотемпературную плазму, вполне можно использовать как оружие. Это будет похоже на очень мощный огнемет (фактически огонь - это тоже плазма). Получается плазма довольно легко - при электрических разрядах, при горении и взрывах, других высокотемпературных воздействиях на вещество.

Интересно, что плазма образуется при функционировании многих давно известных видов оружия. Кумулятивная граната при взрыве формирует мощную струю высокотемпературной плазмы, которая мгновенно делает в толстой броне танка дыру. В рекламных целях такое оружие стали называть плазменным. Взять, к примеру, пресловутые плазменные панели, к которым больше подходит термин «газоразрядные». Скорее, это просто дань хай-теку. Скоро лампы дневного света будет принято называть плазменным освещением, а примус - плазменным нагревателем.

Из новейших средств можно отметить безгильзовую электротепловую химическую пушку. Стреляет она обычными или специальными боеприпасами. По сути, это древняя пушка с запалом. Высоковольтный разряд превращает зажигательную смесь в плазму и выталкивает заряд с огромной скоростью.

Полицейский бесконтактный электрошокер StunStrike компании Xtreme Alternative Defense Systems, в отличие от классических тазеров, не требует дротиков-электродов с проводами. В сторону жертвы выстреливается узкий пучок специальной аэрозоли. Аэрозоль ионизируется, образуя пространственный проводник для высоковольтного разряда. Дальность действия составляет 15 метров.

Среди глобальных идей можно назвать буржуинский проект по формированию многокилометровых ионизированных облаков-плазмоидов в верхних слоях атмосферы. Предполагается, что они будут парализовывать радиосвязь, работу электроники и даже воздействовать на здоровье людей. Аналогичный проект разрабатывается в НИИ Радиоприборостроения под руководством академика Авраменко. Цель наших плазмоидов - создание препятствий на пути ракет и других летящих объектов.

СКАЗОЧНЫЕ ЗВУКИ

Шумовое оружие американцы планировали применить в Ираке. Звуковая пушка Long Range Acoustic Device (LRAD) поражает противника направленным лучом пронзительного визга с уровнем до 130 децибел и частотой от 2 до 3 кГц. Это слегка превышает уровень болевого порога и сравнимо с реактивным двигателем над ухом или концертом Iron Maiden ;-). Ранее подобные установки использовались на военных кораблях для распугивания рыболовецких шхун.

Не утихают споры и вокруг инфразвукового оружия. Колебания воздуха на частотах в диапазоне 3-10 Гц, как известно, могут входить в резонанс с внутренними органами человека, вызывать их вибрацию и повреждения. При этом люди и животные ощущают чувство немотивированного страха и паники. Говорят, где-то в секретных бункерах пытались подобрать частоты для нейтрализации половых органов человека. Такой вариант тоже может в каком-то смысле деморализовать личный состав неприятеля. В любом случае, аэродинамические агрегаты для создания мощного инфразвука будут иметь большие размеры. Воздействие невозможно локализовать в одном направлении. Затыкать уши здесь бесполезно. Поражены будут все, включая оператора установки.

> «...Кучера в асбестовых латах и царевы доезжачие с мотопомпой набросились на обезумевших чудовищ, нанося им удары прикладами лазеров и мазеров».
>
> *Станислав Лем. «Кибериада. Путешествие второе».*

ПУШКИ НА МАГНИТАХ

Немецкий журнал Soldat und Technik недавно поведал о таинственном происшествии в Ираке. Знаменитый американский танк «Абрамс» был прошит насквозь. В обеих стенках башни из суперпрочной антикумулятивной брони образовалось аккуратное отверстие диаметром всего 7 миллиметров! Такое не под силу ни одному оружию на Земле, за исключением... Вывод был таков - либо это инопланетяне, либо так называемая электромагнитная, или рельсовая, пушка. Глава специальной комиссии ЦРУ Чарльз Дефлер подтвердил, что найдены секретные документы, касающиеся проекта создания railgun в Ираке.

Разработка такой пушки велась в США, СССР и других странах с 70-х годов. Установка весит до 100 тонн и имеет длину до 100 метров. Суть механизма проста. По двум направляющим рельсам подается мощный импульс тока. Между рельсами движется тележка-снаряд, которая разгоняется под действием силы Лоренца. Фактически, это линейный электродвигатель постоянного тока. Конструкция должна быть очень точно просчитана, иначе снаряд, не успев разогнаться, испарится под действием огромного наведенного тока.

Технология позволяет разгонять снаряды до гиперзвуковых скоростей. На испытаниях в США были получены скорости более 4 км/с. В перспективе электромагнитные пушки смогут обеспечить метание самонаводящихся снарядов массой около 3 кг на дальность до 5000 км со скоростью 35 км/с. При этом длина пушки составит 45 м. Обычные пороховые заряды на такое не способны даже теоретически. Замечательным свойством рельсовых пушек является высокая скорострельность и способность стрелять очень легкими снарядами. Railgun может на огромном расстоянии «плеваться» кусочками плазмы весом менее одного грамма.

Народной разновидностью электромагнитных пушек являются ружья Гаусса. Они гораздо ближе к квейковской рельсе по габаритам. Принцип действия немного другой. На стволе устанавливается несколько электромагнитных катушек с питанием от предварительно заряженных конденсаторов. Они втягивают снаряд, например гвоздь, последовательно включаясь и отключаясь по мере его прохождения по стволу. Такие ружья могут пробивать бутылки и фанеру. Описаний конструкций в интернете множество, в том числе на сайте][(www1.xakep.ru/post/13054/default.asp). Очень симпатичные пистолеты Гаусса делает Евгений Васильев из Пскова (www.pskovinfo.ru/coilgun).

Railgun на коленке. www.railgun.org

Отечественный пистолет Гаусса

ЗАКЛЮЧЕНИЕ

Побочным продуктом пентагоновских научных изысканий оказалась такая полезная штуковина, как интернет. Я надеюсь, что параллельные мирные открытия, включая мощные источники халявной энергии, похоронят у человечества всякое желание воевать. Беда в том, что вояки будущего растут на сегодняшних компьютерных шутерах. Когда все эти палсганы, шок-райфлы, флэки и прочие бластеры и лазеры станут реальностью, под знамена армии будущего встанут геймеры. Миллионы воинов с великолепными навыками владения новым вооружением и знанием тактики ведения боя в различных условиях. Однажды мир на Земле будет в твоих руках. Дай мне слово: если стрелять, то только по банкам. Из лазера.

Винтовка Corner Shot позволяет стрелять из-за угла. Презентация состоится в Париже 18-21 ноября 2004 года. www.cornershot.com