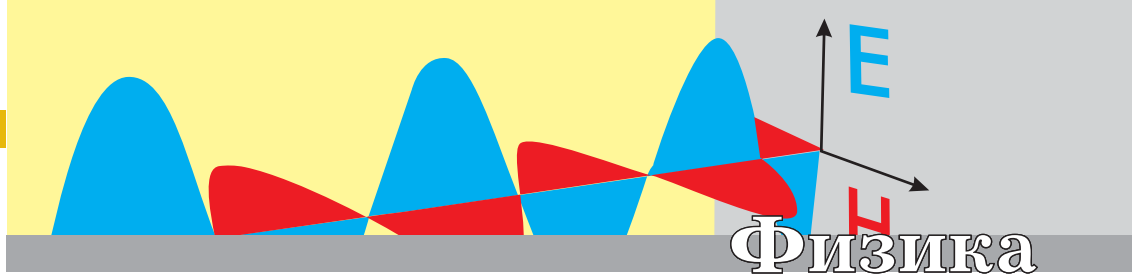


Булюбаш Борис Викторович
Кандидат физико-математических наук, доцент кафедры «Общая и ядерная физика» Нижегородского государственного технического университета им. Р.Е. Алексеева.

«Полупроводниковый терроризм»

В статье рассказывается об угрозе так называемого «технологического терроризма», когда на стадии производства микросхем сознательно нарушается технология их изготовления. Результатом такой формы терроризма может стать внезапный отказ микросхем задолго до истечения гарантийного срока.

Немного истории

В двадцатом столетии в повседневную жизнь человека вошли два изобретения, кардинально эту жизнь изменившие. Мы имеем в виду двигатель внутреннего сгорания (ДВС) и компьютер. Их функции различны: ДВС расширяет прежде всего наши физические возможности, компьютер же является необычайно эффективным инструментом для нашего интеллекта. Эволюция компьютеров – от гигантских сооружений до микропроцессоров – заняла всего несколько десятилетий. Ключевым фактором этой эволюции стала методика изготовления интегральных схем (её основы разработали в конце 50-х гг. англичанин Джефри Димер и американец Джек Килби), позволившая резко уменьшить размеры полупроводниковых устройств. И стоимость компьютеров, и, что не менее важно, их размеры резко снизились благодаря массовому производству микрочипов – крошечных кусочков кремния, с помощью специальной технологии превращённых в комплексы миллиардов транзисторов. В результате, в настоящее время нет такой области человеческой деятельности, в которой не были бы так или иначе задействованы основные компоненты компьютера – микропроцессоры.

Калькулятор Replica 4004 с первым **микропроцессором** Intel. http://habrahabr.ru/page1743/

Проведённый журналом «New Scientist» опрос читателей с просьбой выбрать изобретение, наиболее сильно повлиявшее на развитие цивилизации двадцатого столетия, вывел на первое место (48 процентов голосов) именно микропроцессор. При этом исследование космоса отметило всего три процента опрошенных. Что же касается двигателя внутреннего сгорания, то он уже давно стал для нас привычен и, видимо, именно поэтому не занял в опросе призового места.

Микрочип как угроза американской безопасности

И массовое распространение ДВС, и всеобщая компьютеризация привели к возникновению цивилизационных рисков, предвидеть которые вряд ли было возможно. Массовое распространение двигателей внутреннего сгорания привело к резкому росту концентрации в атмосфере двуокиси углерода, ответственной, в частности, за усиление парникового эффекта и, возможно, за процесс глобального потепления. Что касается общественных рисков, связанных со всеобщей компьютеризацией, то обычно имеют в виду интернет-зависимость, игроманию и т. п. В то же время на уровне же национальной безопасности речь идёт о существенно более серьёзных рисках несанкционированного проникновения в базы данных, рисках хакерских и вирусных атак.

В последние годы, однако, в теме рисков появилось ещё одно измерение. Так, Министерство обороны США проявляет большой интерес к исследованиям в области так называемого технологического терроризма, результатом которого может стать внезапный выход из строя ключевых микросхем и, соответственно, ключевых микропроцессоров.

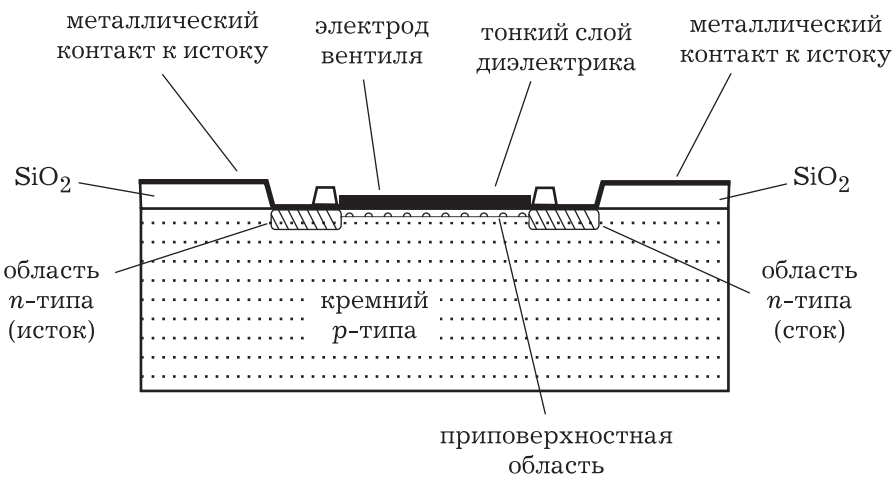
С чем связан такой интерес? В первую очередь с тем, что «благодаря» глобализации разработчик микросхемы и её производитель проживают, как правило, в разных странах. Так, для микроэлектроники США главная сфера деятельности – это конструирование микрочипов, производятся же они в странах с дешёвой рабочей силой, и в итоге Министерство обороны США закупает их в странах Юго-Восточной Азии. Военные весьма озабочены этим обстоятельством. Действительно, внезапный выход из строя микросхемы, встроенной, к примеру, в наводимые системой GPS «умные» бомбы, может вызвать сбой американской системы обороны в критический для страны момент. Подобные угрозы актуальны не только для оборонных систем, но и для энергетических сетей и систем безопасности в управлении дорожным движением.

Возможная методика действий потенциальных технологических террористов была недавно проанализирована группой американских специалистов по физике полупроводников, изложивших результаты своего исследования в так называемом «архиве препринтов». (http://ru.arxiv.org: 0906.3832 и http://ru.arxiv.org: 0906.3834.)

Несколько слов о полевом транзисторе

Для того чтобы понять, как микросхема может стать бомбой замедленного действия, рассмотрим устройство полевого транзистора. Такой транзистор называют также МДП-транзистором; аббревиатура МДП означает «металл – диэлектрик – полупроводник». В таком транзисторе слой металла сменяется слоем диэлектрика и затем слоем полупроводника. МДП-транзисторы потребляют относительно немного энергии, их активно используют в ждущих и следящих устройствах. Самые распространённые бытовые приборы с такими транзисторами – это наручные кварцевые часы и пульт дистанционного управления для телевизора. Именно полевые транзисторы являются основным элементом микросхем памяти, процессора и т. д. Благодаря интегральной технологии на одном чипе площадью в 1-2 $см^2$ уже сейчас удаётся разместить до нескольких миллиардов таких транзисторов.

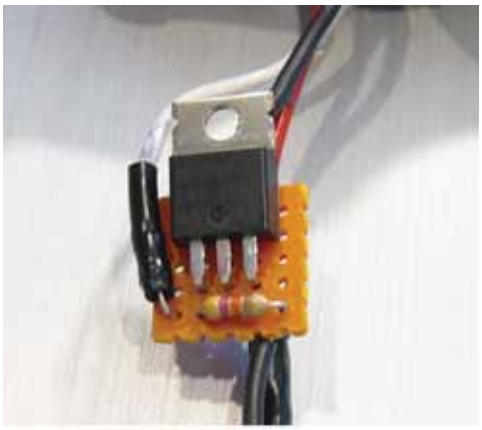
Как происходит усиление сигнала в МДП-транзисторе? В так называемой подложке – полупроводниковом кристалле (обычно кремниевом), характеризующемся относительно высоким удельным сопротивлением, формируются две пространственно удалённых друг от друга области, в которых тип проводимости противоположен типу проводимости подложки. Пусть, к примеру, проводимость в подложке обеспечивают электроны (n-тип проводимости). Тогда указанные области имеют p-тип проводимости; иначе говоря, протекание электрического тока в них обеспечивается дырками. Если же p-тип проводимости характерен для подложки, то в данных областях за электрический ток «отвечают» электроны. На эти области, разделённые расстоянием порядка микрона, наносятся два металлических электрода. Их называют исток (source) и сток (drain). Саму же поверхность подложки с помощью технологии высокотемпературного окисления покрывают изолирующим слоем диэлектрика (как правило, двуокисью кремния SiO_2). На изолирующий слой помещают также третий электрод полевого транзистора, его называют затвором, или, иногда, вентилем (gate).



Схематическое устройство МДП-транзистора.
http://www.intuit.ru/department/hardware/intsensors/10/

Пусть подложка имеет дырочную проводимость, а на затвор подан положительный (относительно подложки) потенциал. В этом случае свободные электроны под действием электрического поля начнут двигаться в сторону затвора. Их концентрация на границе подложки и изолирующего слоя начнёт, таким образом, расти. В итоге вблизи верхней границы подложки появится проводящий канал, соединяющий друг с другом два других электрода – исток и сток. Если изменить поданный на затвор потенциал, то проводимость канала изменится. Именно это обстоятельство позволяет использовать полевой транзистор в качестве усилителя. Действительно, небольшие колебания напряжения на затворе приведут в этом случае к существенным изменениям силы тока в проводящем канале между истоком и стоком. Если же на затвор подан отрицательный относительно подложки потенциал, то проводящий канал не сформируется и ток в цепи исток – сток не появится. Таким образом, при изменении полярности напряжения на затворе полевой транзистор работает как переключатель.

По целому ряду причин параметры полевого транзистора со временем ухудшаются. Если при производстве микросхемы соблюдены все технологические требования, то микросхема прослужит достаточно долго: характеристики транзисторов существенно ухудшатся приблизительно лет за десять. Потенциальный террорист должен обладать весьма высокой квалификацией, чтобы суметь внести такие изменения в технологию изготовления микросхем, из-за которых скорость процессов деградации параметров транзистора существенно вырастет. Если ему удастся это сделать, то микросхема выйдет из строя существенно раньше своего гарантийного срока: это может произойти через год (или через несколько месяцев). Разумеется, перестанет работать и тот микропроцессор, частью которого данная микросхема является.



Установка **полевого транзистора**. http://www.airsoft.mk.ua/forum/index.php?topic=14.0

Инжекция горячих носителей как оружие террориста

Один из тех физических процессов, которые ухудшают параметры МДП-транзисторов, является «инжекция горячих носителей» (hot carrier injection). Горячими носителями в физике полупроводников называют электроны и дырки, которые приобрели под действием электрического поля достаточно большую энергию («разогрелись»). Под инжекцией же понимают проникновение таких носителей в изолирующий слой оксида кремния. По понятным причинам характеристики полевого транзистора при этом ухудшаются. Из-за инжекции горячих носителей полевые транзисторы могут, к примеру, начать нестабильно работать при низких температурах. Почему это происходит? Потому что с понижением температуры у электронов возрастает средняя

длина свободного пробега и они успевают ускориться под действием электрического поля до бóльших, нежели раньше скоростей. Скорость инжекции при этом возрастает. Обычно же твердотельные устройства начинают нестабильно работать с увеличением температуры, но не с её понижением.

Авторы публикаций на сайте препринтов напоминают, что для предохранения изолирующего слоя от разрушения его насыщают окисью азота. Это означает, что технологу достаточно уменьшить концентрацию азота (либо слегка изменить температуру процесса насыщения) – и в том, и в другом случае проницаемость слоя для «горячих» дырок (либо электронов) станет больше, и цель террористов будет достигнута.

Казалось бы, нарушение технологии производства микросхемы можно легко обнаружить – например, при контрольной проверке изготовленных микросхем. Такое тестирование, однако, должно носить массовый характер; по этой причине оно должно быть недорогим и не занимать много времени. Обнаружить же за небольшой промежуток времени ускорение инжекции электронов и дырок, а также и незначительное снижение электроизолирующих свойств оксида кремния вряд ли возможно.

Угрозы, связанные с технологическим терроризмом, начинают признавать в правительственных структурах США. Так, журнал «New Scientist» ссылается на заявление полковника Гленна Циммермана (Glenn Zimmerman) из специального отдела Пентагона по кибервойнам (Pentagon's Cyber Command for computer warfare). Имея в виду опасности технологического терроризма, Циммерманн заявил недавно о необходимости тщательно проверять наиболее важные микросхемы, заметив, что США импортируют большую часть используемых полупроводниковых приборов, «а потому и сами эти приборы, и технология их производства должны быть подвергнуты процедуре всесторонней сертификации».

Тот факт, что угроза технологического терроризма стала активно обсуждаться в экспертном сообществе, является наглядной иллюстрацией изменений во взаимоотношениях науки и общества, о которых писал недавно в газете «Троицкий вариант» к. ф.-м. н. Дмитрий Баюк, с. н. с. Института истории естествознания и техники РАН им. С.И. Вавилова. По его словам, «наука вновь меняется вслед за меняющимся миром, и не просто изменяет его, а обеспечивает само его существование». Происходит это потому, что «общество начинает осознавать стоящие перед ним опасности, в том числе те, которые возникли в силу его же собственного развития». Среди угроз современной техногенной цивилизации – и уязвимость земных энергосистем воздействию магнитных бурь, и истощение озонового слоя, и рост концентрации парниковых газов. Теперь же мы не должны забывать также и об угрозах, спрятанных в микросхемах.