УДК 621.38; 53.082
DOI: 10.33764/2618-981X-2019-6-1-108-114

ИССЛЕДОВАНИЕ ПРОЦЕССА ФОРМИРОВАНИЯ СУБМИКРОННЫХ ЭЛЕМЕНТОВ ОПТОЭЛЕКТРОННЫХ УСТРОЙСТВ С УЧЕТОМ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Анатолий Александрович Ильченко
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (983)128-22-26, e-mail: Tolik212171@gmail.com

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой информационной безопасности, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

В работе рассмотрен термин «аппаратная закладка», указаны критические этапы производства микросхем, на которых могут возникнуть закладки, описаны возможные последствия активирования закладки. Также описан способ, не допускающий появления закладок, на примере импортозамещения. Показан разработанный технологический режим получения субмикронных элементов на примере слоя поликремния.

Ключевые слова: аппаратная закладка, безмасковая фотолитография, нанесение фоторезиста, информационная безопасность, конструктивные различия, поликремний.

RESEARCH OF FORMATION PROCESS OF SUBMICRON ELEMENTS OF OPTOELECTRONIC DEVICES CONSIDERING INFORMATION PROTECTION REQUIREMENTS

Anatoly A. Ilchenko
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone (983)128-22-26, e-mail: Tolik212171@gmail.com

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Information Security, phone: (903)937-27-90, e-mail: i.n.karmanov@ssga.ru

In this paper, the term «hardware tab» is reviewed, critical stages of chip production on which tabs can occur are indicated, the possible consequences of tab activation are described. Also a method is described that does not allow the appearance of tabs, as an example of import substitution. The developed technological mode of submicron elements obtaining is shown, by the example of a polysilicon layer.

Key words: hardware tab, maskless photolithography, photoresist application, information security, design differences, polysilicon.

Введение

Сложно представить жизнь современного человека без использования различных электронных устройств, будь то смартфон, фотоаппарат, карта оплаты

проезда в транспорте и др. Все современные цифровые устройства построены на базе интегральных схем (далее ИС). Безопасность информации является одной из основных характеристик любых электронных устройств [1].

Опасность утраты или утечки информации существует как на программном, так и на аппаратном уровне. Рассмотрим, каким образом возникают уязвимости на аппаратном уровне.

Поскольку количество электронных устройств постоянно растет, производители ИС стали применять новые подходы к производству, способные обеспечить спрос. Выделяют три группы компаний, производящие ИС [2].

Первая группа. Компании, имеющие собственные производства и отдел разработки микросхем. Используя данный подход изготовления микросхем, появляется возможность исключить уязвимости на аппаратном уровне (так называемые закладки в микросхемах), так как производитель контролирует все этапы производства ИС.

Вторая группа. Компании, которые не имеют собственных производственных мощностей. Они занимаются разработкой ИС, полученную информацию передают в компании, которые занимаются производством. Данный подход позволяет уменьшить производственные издержки, но он же создает опасность модификации передаваемой в производство информации с целью добавления в устройство аппаратных закладок.

Третья группа. Компании, занимающиеся только производством, у них отсутствует отдел собственной разработки [3].

Стоить отметить, что современная разработка ИС происходит не «с нуля», разработчики покупают готовые IP блоки. Это отдельная часть микросхемы, выполняющая определенную функцию. Собственно, аппаратные закладки, могут быть внедрены в IP блоки, что ставит под угрозу готовое устройство [4].

Что же представляет из себя аппаратная закладка в ИС? Исследователи из МТИ опубликовали доклад, в котором описали процесс изготовления аппаратных закладок на физическом уровне. В основе процесса лежит метод изменения полярности легирующей примеси на определенных участках транзистора. После внедрения подобной закладки инвертер будет выводить плюс напряжения вне зависимости от напряжения на входе. Примером реально полученной подобной аппаратной закладки может служить генератор псевдослучайных чисел в процессоре Intel Ivy Bridge, генерирующий 128-битные псевдослучайные числа, которые, благодаря наличию закладки, оказываются легко предсказуемыми [5].

Обнаружение подобных закладок проблематично, поскольку изменениям подвергаются слои легирования, которые не видны при микроскопии.

В зависимости от целей, преследуемых злоумышленником, некоторые закладки должны всегда находиться во включенном состоянии; другие же, наоборот, должны быть неактивны до определенного момента. Можно выделить две основные категории аппаратных закладок, отличающиеся способом активации – активные всегда и активирующиеся по событию. Аппаратные закладки, принадлежащие к первой категории, активированы постоянно – как это видно из названия; они могут влиять на схему в любой момент времени. Условия, ак-

тивирующие закладки второго типа, специально делают маловероятными, чтобы избежать случайного включения при тестировании или использовании схемы.

Как было отмечено выше, для минимизации рисков внедрения аппаратных закладок, необходимо свести процесс изготовления и разработки на одном предприятии. В Новосибирске разработкой и выпуском ИС занимается АО «НПП «Восток». Данное предприятия имеет полный цикл производства и разработки ИС, что позволяет изготавливать ИС для использования в военной технике и электронных устройствах, требующих повышенного внимания к информационной безопасности. Но для улучшения компонентной базы и увеличения вычислительных способностей ИС необходимо увеличивать количество логических элементов (транзисторов), для чего требуется уменьшать размер дискретного транзистора.

Методы и методики

В данной работе описывается процесс получения элементов субмикронного размера на маске из фоторезиста, методом безмасковой фотолитографии [6].

Чтобы получить элемент субмикронного размера, необходимо:

– на подложку (кремневая пластина) равномерно нанести слой фоторезиста с разрешающей способностью, обеспечивающей субмикронный размер, имеющего пик чувствительности вблизи длины волны используемого излучения;

– определить технологические параметры, обеспечивающие искомый результат (мощность излучения, смещения точки фокуса, время проявления).

Для достижения результата применялась технология безмасковой фотолитографии. Особенность данного метода заключается в том, что экспонирование производится без участия фотошаблонов, и элементы формируются методом модулирования лазерного излучения на подложку [7].

На рис. 1 показана структурная схема установки безмасковой фотолитографии.

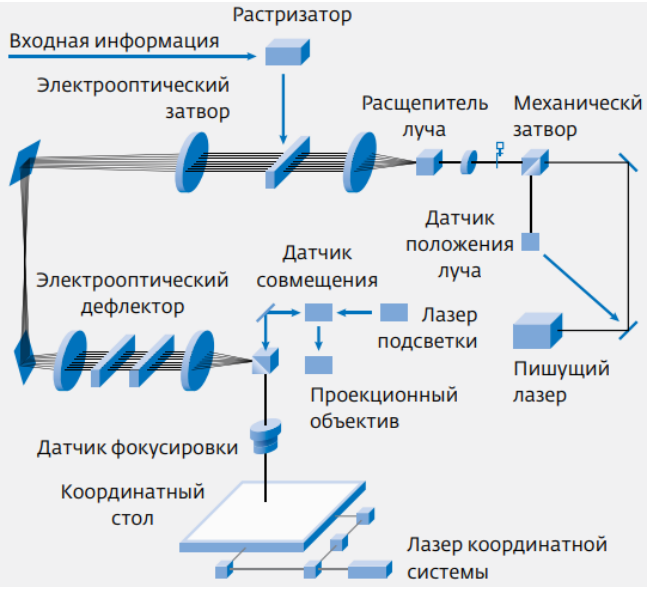

Рис. 1. Структурная схема установки безмасковой фотолитографии

Результаты

Для получения светочувствительной пленки был выбран фоторезист SPR 700, поскольку он имеет необходимую разрешающую способность и светочувствительность [8].

Предприятие «НПП «Восток» ранее не использовало данную марку фоторезиста, вследствие чего было необходимо разработать режим нанесения равномерной пленки толщиной 1 мкм ± 10 нм.

На рис. 2 представлена зависимость толщины светочувствительного слоя от скорости вращения центрифуги [9].

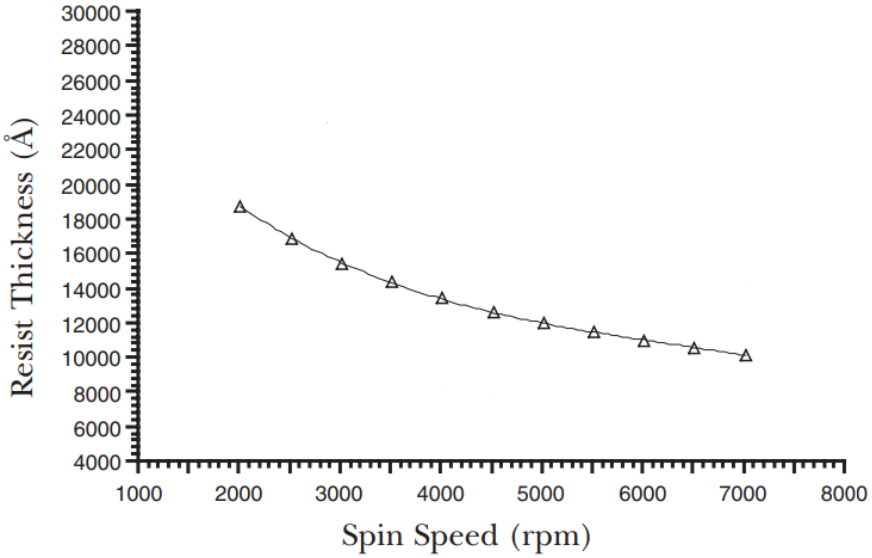

Рис. 2. Зависимость толщины светочувствительного слоя от скорости вращения центрифуги

Варьируя такие параметры, как скорость вращения центрифуги, ускорение вращения, время подачи фоторезиста, был разработан режим, обеспечивающий нанесение качественной фоторезистивной пленки.

На рис. 3 представлен разработанный технологический режим.

Поскольку фотомаска нужна для проведения последующих операций, таких как травление, легирование и др., то была выбрана подложка со слоем поликремния, на который был нанесен фоторезист, для последующего проведения плазмохимического травления. Из поликремния изготавливают затворы полевых транзисторов [10].

Для разработки технологического режима экспонирования и проявления необходимо подобрать мощность экспонирования, смещения точки фокусировки, и время проявления. Если использовать большую мощность экспонирования, либо большее время проявления, то получаемые элементы будут искажаться, как изображено на рис. 4.

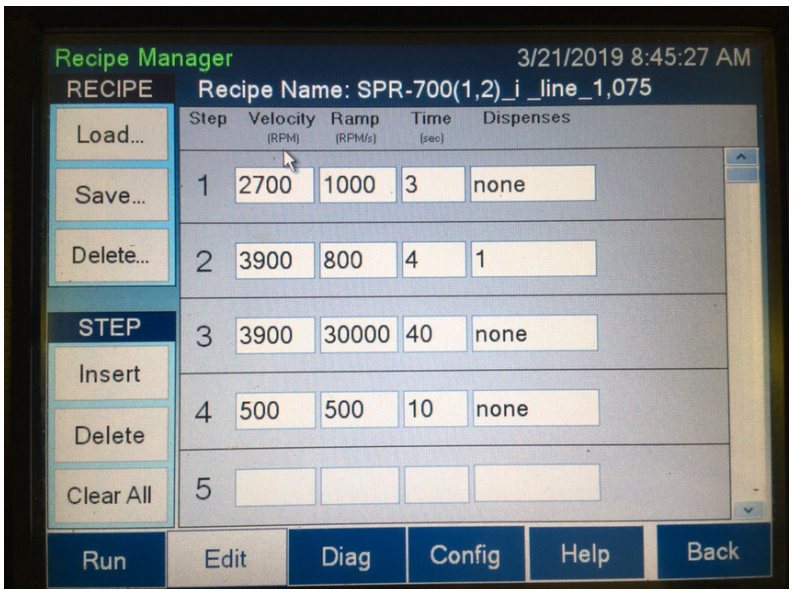

Рис. 3. Разработанный режим нанесения фоторезиста

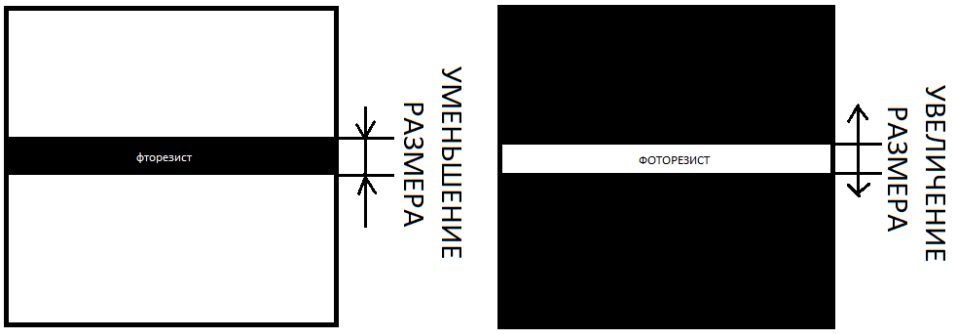

Рис. 4. Изменение размеров элементов

В качестве времени проявления использовалась константа в 30 секунд.

В ходе разработки технологического режима изменялась только мощность экспонирования. Для нахождения оптимальной мощности использовался режим, в котором на пластине производится экспонирование матрицы, где каждый элемент экспонируется со своей мощностью. Таким образом, при контроле в оптический микроскоп находится визуально наилучший элемент, а мощность, с которой он был изготовлен, принимается за оптимальную. При выполнении данной работы использовалось значение мощности лазера 115 мВт. Параметры фокусировки изменениям не подвергались.

На рис. 5 и 6 показан результат экспонирования. На рис. 7 и 8 показан результат травления поликремния. Таким образом, был получен режим экспонирования фоторезиста методом безмасковой фотолитографии, обеспечивающий получение элементов субмикронного размера.

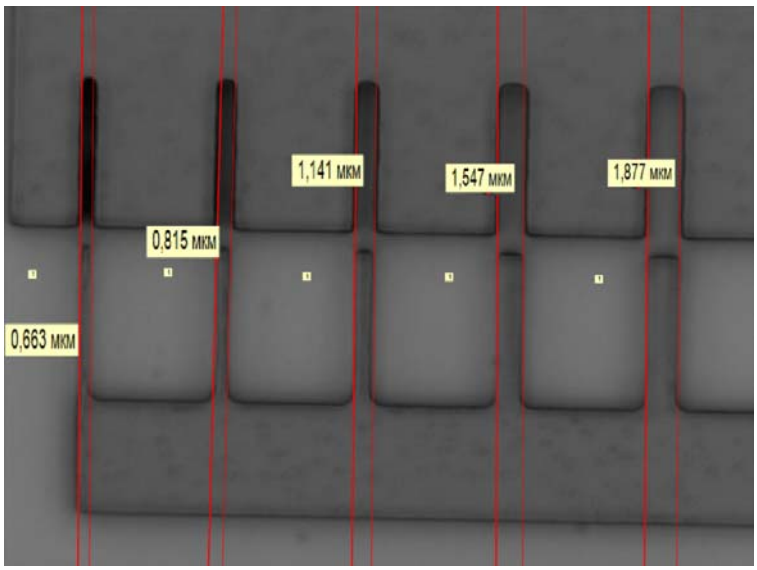

Рис. 5. Контрольные размеры

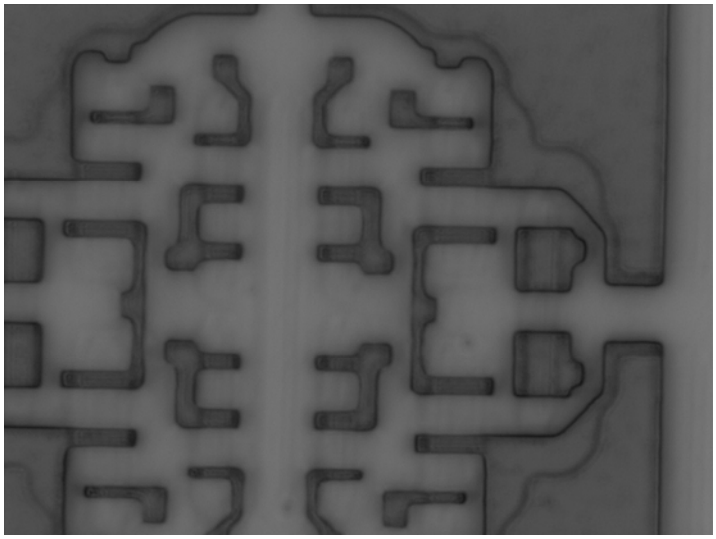

Рис. 6. Рабочие затворы

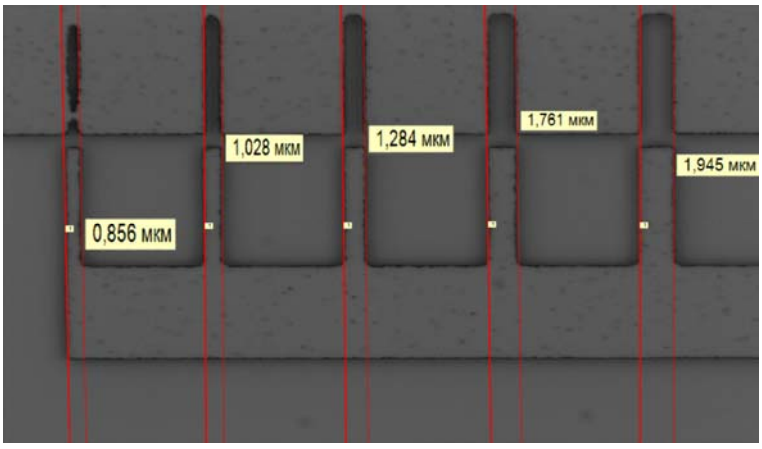

Рис. 7. Результаты травления

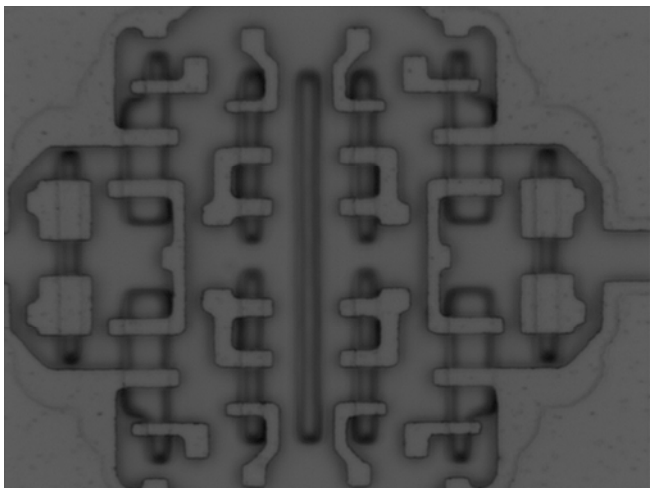

Рис. 8. Результаты травления

Заключение

Вредоносное аппаратное обеспечение действительно является серьезной проблемой безопасности электронных устройств, особенно, если речь идет о выполнении критически важных задач государственного уровня. Разработка новых технологических режимов и внедрение их в производство является одной из важнейших задач для обеспечения информационной безопасности электронных устройств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Defense Science Board. Report of the Defense Science Board Task Force on High Performance Microchip Supply. US DoD, February 2005.
2. G.T. Becker, F. Regazzoni, C. Paar, W.P. Burleson. Stealthy Dopant level Hardware Trojans. International Conference on Cryptographic Hardware and Embedded Systems, ser. CHES. Berlin, Heidelberg: Springer Verlag, 2013.
3. SypherMedia International. Circuit Camouflage Technology – SMI IP Protection and Anti Tamper Technologies. White Paper Version 1.9.8j, March 2012.
4. H. Li, Q. Liu, J. Zhang. A survey of hardware Trojan threat and defense, 2016.
5. M. Tehranipoor, C. Wang, editors. Introduction to Hardware Security and Trust. Springer, 2012.
6. Валиев К. А., Раков А. А. Физические основы субмикронной литографии в микроэлектронике. – М. : Радио и связь, 1984. – 349 с.
7. Введение в нанотехнологию / Н. Кобаяси, под ред. проф. Л. Н. Патрикеева. – М. : Бином. Лаборатория знаний, 2008. – 134 с.
8. Введение в фотолитографию / Ю. С. Боков [и др.], под ред. В. П. Лаврищева. – М. : Энергия, 1977. – 400 с.
9. Гусев А. И. Наноматериалы, наноструктуры, нанотехнологии. – М. : Наука-Физматлит, 2007. – 416 с.
10. Процессы микро- и нанотехнологии : учеб. пособие / Т. И. Данилина [и др.]. – Томск : Гос. ун-т систем упр. и радиоэлектроники, 2005. – 315 с.

© А. А. Ильченко, И. Н. Карманов, 2019