de los productos agrícolas y el de las manufacturas y servicios con uso intensivo de mano de obra (por ejemplo, la construcción), en los cuales los países en desarrollo tienen una ventaja comparativa.

Los países industriales mantienen una fuerte protección de la agricultura mediante un sistema de aranceles muy elevados que incluye máximos arancelarios, progresividad arancelaria y contingentes arancelarios restrictivos.

En los países industriales el sector manufacturero está poco protegido en términos generales, pero siguen existiendo barreras elevadas contra muchos productos que exigen un uso intensivo de la mano de obra y provienen de países en desarrollo.

Muchos países en desarrollo tienen aranceles altos: los que traban la importación de productos industriales son, en promedio, tres o cuatro veces más elevados que los que existen en los países industriales y tienen también máximos y progresividad. Los aranceles agrícolas son aun mayores (18%) en los países en desarrollo que en los industriales.

Por distintas razones, los sistemas de acceso preferencial para los países más pobres no han logrado ampliar muy bien el acceso a los mercados. A menudo excluyen a los productos muy protegidos que más interesan a los exportadores de esos países, o les ofrecen beneficios menos generosos. Suelen ser complejos falto de transparencia, y por lo general están sujetos a diversas exenciones y condiciones (algunas no económicas) que ponen límite a los beneficios o los suprimen una vez logrado un acceso significativo al mercado.

***Сыропущинский Д.В.***
**Научный руководитель Мардыко М.Н.**

*Интернет стал не только новой стороной жизни, но и местом, где совершаются преступления. Число компьютерных преступлений увеличивается с каждым годом. Компании ежегодно тратят громадные деньги на обеспечение своей информационной безопасности. В докладе рассматриваются основные источники угрозы и меры по борьбе с ними, которые предлагают эксперты.*

## CIBERDELINCUENCIA

El término ciberdelincuencia resume una oscura amenaza que afecta a la economía digital y se está convirtiendo en el tema más debatido en la política de seguridad.

Las principales amenazas que perciben las empresas son los virus, la destrucción de datos y la piratería. Aparte de los creadores de virus son principalmente los denominados script kiddies y black hat hackers quienes traen de cabeza a las empresas en red. Con este término designan a los jóvenes usuarios de Internet que desconocen las técnicas de los hackers y se limitan a utilizar programas automatizados con intenciones fraudulentas.

El número de objetivos susceptibles de ser atacados por un hacker equivale a toda la tecnología de la red: servidores web, ordenadores centrales o aplicaciones, así como también routers y switches con los que está dirigido el tráfico de datos por Internet o por una red privada. El software empleado por los administradores de redes para controlar sus servidores es el mismo que utilizan los atacantes.

La mayoría de los grupos industriales prefiere no desvelar los pormenores de las medidas de seguridad de sus sistemas informáticos. Ya se trate de empresas de armamento, líneas aéreas o bancos, en toda Europa se escuchan las mismas declaraciones estereotipadas: que la seguridad es una parte importante de la concepción TI, que afecta al grupo empresarial en su conjunto y que se le están dedicando unos recursos financieros y de personal importantes. Las empresas deben asumir la responsabilidad de proteger sus recursos digitales. En la vida real, nadie deja abierta la puerta de su negocio una vez terminado el horario de apertura, con la esperanza de que la policía se ocupe de vigilarlo. Los recursos disponibles para defender las redes de las empresas se han vuelto tan accesibles que el sector empresarial puede autoprotegerse de forma eficaz.

Pero los actos de espionaje, sabotaje y fraude son fáciles de cometer en una red que se concibió como medio de comunicación, y no como «vía de alta seguridad». El diseño fundamental de la red tiene múltiples agujeros, está siempre atenta y constantemente descubre nuevas lagunas o diseña nuevas herramientas de ataque.

Con todo, los esfuerzos del mundo empresarial por combatir la ciberdelincuencia son insuficientes. Los políticos piden una

ampliación de las atribuciones de los investigadores en el marco internacional. En este sentido, la propuesta más completa de cara a limitar la ciberdelincuencia es la presentada por el Consejo de Europa. Con este acuerdo se pretende perseguir mejor en el plano internacional un amplio abanico de infracciones penales relacionadas con los ordenadores. El borrador incluye disposiciones relativas a la entrada en sistemas informáticos, la transmisión de material pornográfico infantil y los fraudes cometidos con ayuda de un ordenador, pero sobre todo, se trata de prohibir las herramientas de piratería informática que, por cierto, también utilizan los administradores para comprobar la seguridad de sus sistemas.

***Целюк А.С.***
**Научный руководитель Мардыко М.Н.**

*Введение в обращение единых европейских банкнот и монет – важное событие в монетарной истории. Оно составляет финальную стадию в переходе к единой европейской валюте и выведении из обращения национальных денежных единиц стран-членов Европейского Валютного Союза. Этот процесс вызвал ряд опасений, связанных с различиями в развитии отдельных сфер жизни общества рвзных европейских стран, и их влиянии на дальнейшее развитие экономики и интеграционных процессов в Европе.*

## ENTRADA DEL EURO FÍSICO: CONSECUENCIAS Y PROBLEMAS

Del efecto de la entrada del euro físico se esperaba que pudiera subir el tipo de cambio del euro, crecer drásticamente tanto el comercio interior de la zona euro como la misma economía europea, que los precios llegan a convergencia.

Al mismo tiempo tenían miedo que pudiera frenar el desarollo económico tras los costes del cambio, incentar la inflación tras multiples redondeos de los precios al alza, aparecer un gran volúmen del efectivo negro; provocar el descontento de los ciudadanos que no estan satisfechos con las discrepancias en los precios.