

## КИБЕРБЕЗОПАСНОСТЬ: ВОПРОСЫ, ПРОБЛЕМЫ И УГРОЗЫ БЕЗОПАСНОСТИ

*Исаичкина С.В.*

*Белорусский государственный университет информатики и радиоэлектроники  
г. Минск, Республика Беларусь*

*Жилинская Н.Н. – к. э. н, доцент*

Сегодня киберпространство и уровень развития ИТ дают уникальные возможности для управления технологическими процессами в государственных инфраструктурах, в том числе и оборонных, в энергетике, на транспорте, в банковской и многих других сферах экономической деятельности.

Киберпространство включает в себя три основные составляющие:

Информация

Техническая инфраструктура, ИТ, ПО

Информационное взаимодействие субъектов

В связи с развитием ИТ возникает так называемая киберпреступность. Сегодня компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства.

Сегодня мы можем приобрести большинство товаров с помощью Интернета. Приобретение билетов в театр, кино, на поезд или самолет через Интернет становится для нас обычным делом. Заработную плату нам перечисляют на банковские карты. Оплачивать покупки мы также можем с помощью карты. Тем самым мы становимся зависимыми от компьютеров.

В связи с этим обостряется проблема информационной безопасности. Возможности технологий начинают активнее использоваться в преступных целях.

Под кибератакой понимают любую попытку несанкционированного доступа к отдельному компьютеру или компьютерной сети.

Причины существования:

прибыльность

простота исполнения

низкий уровень риска

появление новых сервисов

информационные войны

Особенности киберпреступлений:

скрытность преступления.

преступления носят трансграничный характер.

частое обновление способов совершения преступлений.

преступление может быть совершено в нескольких местах одновременно.

потерпевшие могут не догадываться, что они подверглись преступному воздействию.

киберпреступления носят дистанционный характер

К типам угроз кибербезопасности относятся

вредоносное ПО

социальная инженерия

программы-вымогатели

фишинг

последствия кибератак:

временная потеря доступа к важной деловой информации

временная остановка бизнес-процессов

потеря контактов

ущерб репутации компании

повышение страховых взносов

аспекты информационной безопасности:

доступность (возможность за разумное время получить требуемую информационную услугу)

целостность (защищенность от искажения информации и ее подмены)

конфиденциальность (защита от похищения конфиденциальной информации и ее распространения)

Основные компоненты, которые необходимо защитить:

интеллектуальные устройства и маршрутизаторы

компьютеры

сети и облачная среда  
Наиболее распространенными технологиями, которые используют для защиты перечисленных компонентов, являются  
защита от вредоносного ПО  
фильтрация DNS  
антивирусное ПО  
межсетевые экраны

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак.

Ежегодно экспертами Международного союза электросвязи ООН составляется рейтинг стран по уровню кибербезопасности.

Глобальный индекс кибербезопасности (GCI) отражает уровень киберзащищенности государств и усилия, которые прилагает страна для улучшения этого показателя.

В 2017 году Беларусь заняла 39 позицию в мире и 3 среди стран СНГ.

К мировым лидерам по уровню кибербезопасности эксперты отнесли Сингапур, США, Малайзия, Эстония и Оман.

Таблица 1. Три лучшие страны в рейтинге СНГ

Страна	Индекс	Правовое поле	Техническое поле	Организационное поле	Потенциал	Сотрудничество
Грузия	0.81	0.91	0.77	0.82	0.9	0.7
Россия	0.78	0.82	0.67	0.85	0.91	0.7
Беларусь	0.59	0.85	0.63	0.33	0.68	0.47

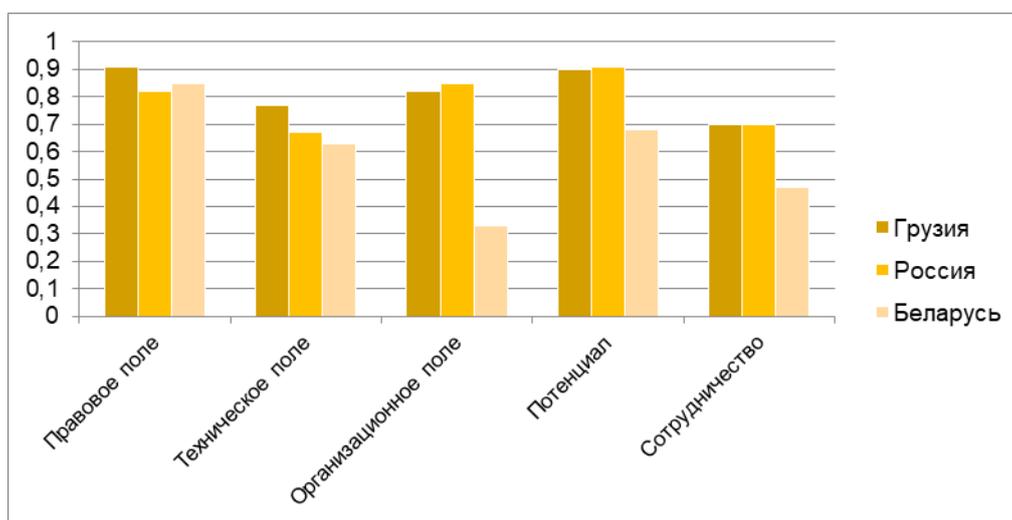


Рисунок 1 – Три лучшие страны в рейтинге СНГ

**Список использованных источников:**

1. <http://xbb.uz/IT/Kiberataki-ponjatje-celi-posledstviya-i-mery-protivodejstvija>
2. <https://nonews.co/directory/lists/countries/cybersecurity-index>
3. [https://www.cisco.com/c/ru\\_ru/products/security/what-is-cybersecurity.html](https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html)

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ЭФФЕКТИВНЫЙ СПОСОБ ПОДБОРА ПЕРСОНАЛА

*Ковбаса Г. А., Юревич В. С.*

*Белорусский государственный университет информатики и радиоэлектроники  
г. Минск, Республика Беларусь*

*Ермакова Е.В. – к.э.н., доцент*

В настоящее время широко распространена автоматизация различных процессов. Это также затронуло такую сферу человеческой деятельности, как рекрутинг. В данной работе рассмотрены способы использования систем на основе искусственного интеллекта в рекрутинге, а также связанные с этим риски.