УДК 001.11

Кодиров Зохид Зокирханович
Наманганский инженерно-строительный институт
преподаватель кафедры «Информационные системы и технологии»
Республика Узбекистан, город Наманган

Исмоилов Элмуродхўжа Тўхтасинхўжа ўгли
Наманганский инженерно-строительный институт
студент кафедры «Информационные системы и технологии»
Республика Узбекистан, город Наманган

КИБЕРБЕЗОПАСНОСТЬ – КАК ТРЕБОВАНИЕ ВРЕМЕНИ

Аннотация: *В статье раскрываются проблемы кибербезопасности в Узбекистане. Республике Узбекистан планомерно осуществляются мероприятия по обеспечению защиты информации в средствах ИКТ. Следует также отметить, внимание руководства страны к обеспечению кибербезопасности в Республике Узбекистан.*

Ключевые слова: *Кибербезопасность, киберугрозы, кибер атака, защита информации.*

Kodirov Zohid Zokirkhanovich
Namangan Institute of Engineering and Construction
teacher of the Department "Information Systems and Technologies"
Republic of Uzbekistan, city of Namangan

Ismoilov Elmurodxo‘ja To‘xtasinxo‘ja o‘g‘li
Namangan Institute of Engineering and Construction
student of the Department "Information Systems and Technologies"
Republic of Uzbekistan, city of Namangan

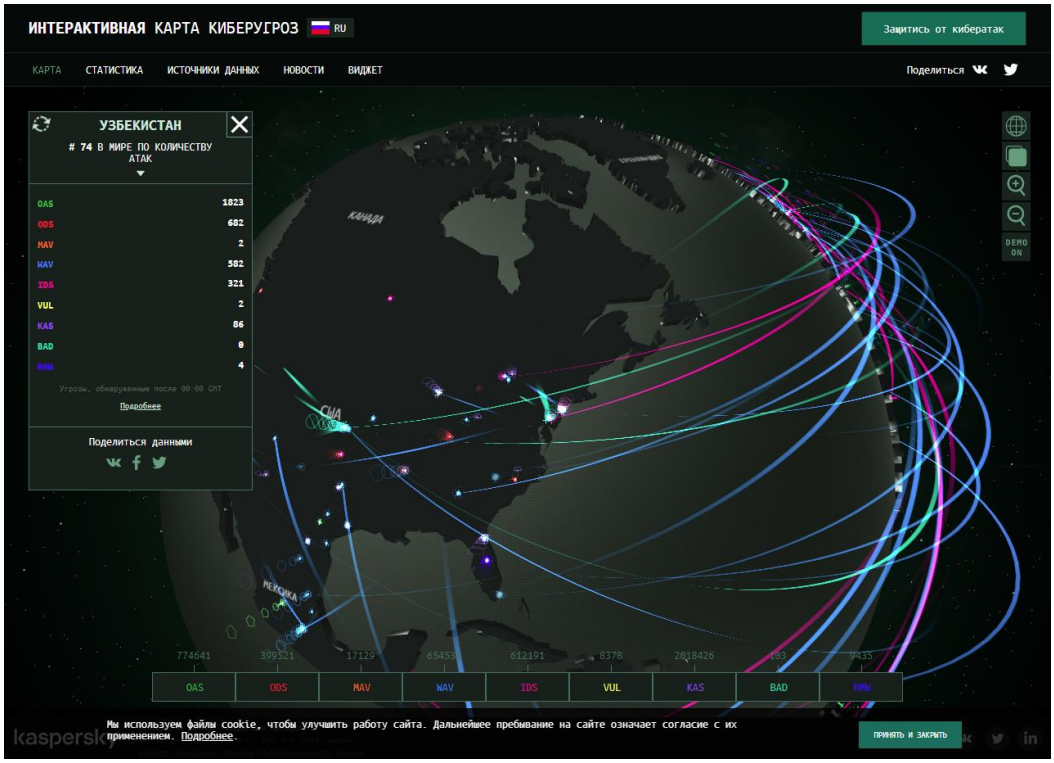
CYBERSECURITY – AS A REQUIREMENT OF THE TIME

Abstract: *The article reveals the problems of cybersecurity in Uzbekistan. The Republic of Uzbekistan is systematically implementing measures to ensure the protection of information in the ICT media. It should also be noted that the attention of the country's leadership to ensuring cybersecurity in the Republic of Uzbekistan.*

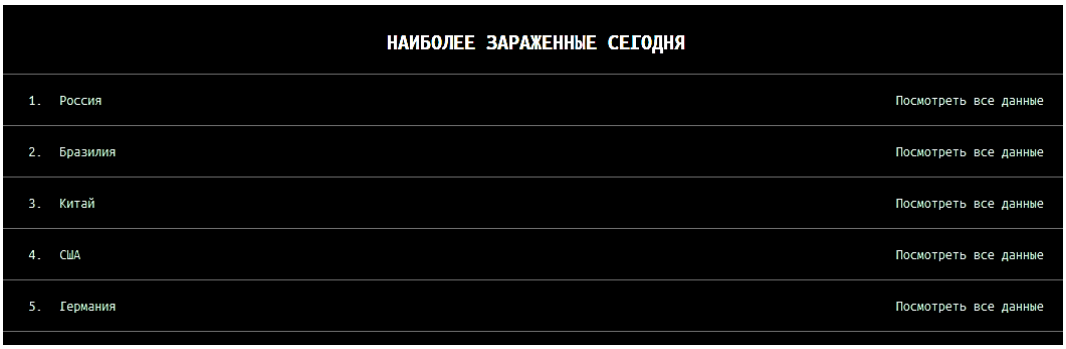
Keywords*: Cybersecurity, cyber threats, cyber attack, information protection.*

Кибербезопасность – это один из основных глобальных рисков мирового сообщества, стоящих в одном ряду – угрозы терроризма, глобальное потепление, рост популизма и торговые войны.

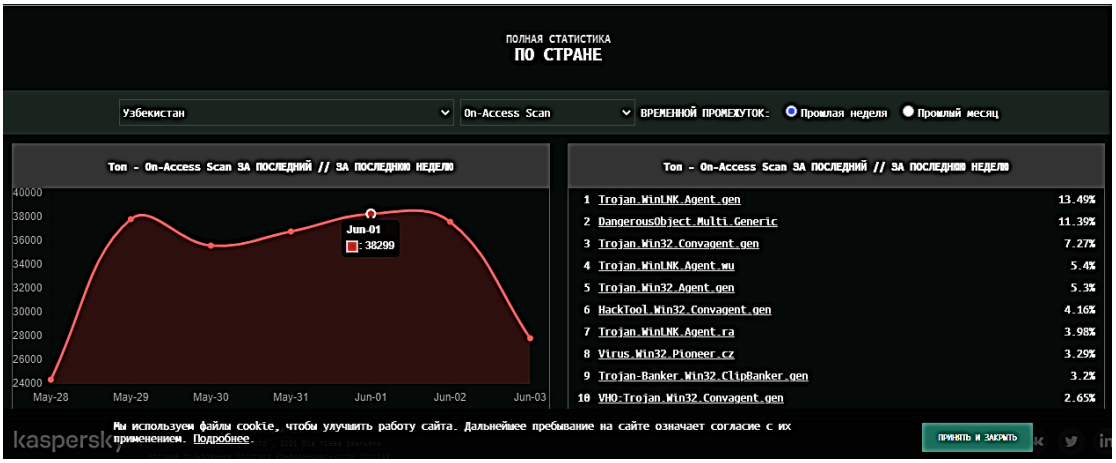
При этом, мировая практика последних лет показывает, что шансы на успешное расследование киберпреступлений составляет всего 0,05%! Между тем, предполагаемый ущерб от киберпреступлений обойдется, по мнению экспертов, мировой экономике в 6 триллионов долларов США уже в 2023 году. Для сравнения, это в два раза больше, чем зарабатывает преступный мир за счет «традиционных» преступлений: наркоторговля, грабежи, продажа оружия и т.п.



Так, по данным интерактивной карты киберугроз лаборатории Касперского, по количеству атак на информационное пространство, по состоянию на июнь 2023 г. Узбекистан занимает 51 место. На первом месте находится Россия, на втором Бразилия, на третьем месте Китай, на четвертом месте США и на пятом месте Германия.



Необходимо отметить, что только за неделю с 28 мая до 3 июня 2023 года в отношении Узбекистана осуществлено в среднем 38299 сетевых атак.



В этой связи, принимая во внимание остроту сложившейся ситуации, в Республике Узбекистан планомерно осуществляются мероприятия по обеспечению защиты информации в средствах ИКТ. Следует также отметить, внимание руководства страны к обеспечению кибербезопасности в Республике Узбекистан.

Так, в период с 2018 по 2020 годы приняты один Указ и три Постановления Президента Республики Узбекистан в сфере обеспечения кибербезопасности, последним из которых (ПП-4751 от 15.06.2020 г.) определено создание Государственной системы защиты информационных систем и ресурсов Республики Узбекистан.

Этим же законодательным актом ГУП «Центр кибербезопасности» объявлен рабочим органом по созданию, обеспечению функционирования и развитию технической инфраструктуры Государственной системы защиты информационных систем и ресурсов Республики Узбекистан.

В последнее время в Интернете набирают популярность новые методы хищения денег с пластиковых карт путем обмана наших соотечественников, с целью легкого заработка.

В целях предостережения наших граждан от посягательств киберпреступников, сохранения их персональных данных и финансовых сбережений, хотелось бы напомнить о соблюдении простых правил:

- Не сообщать секретные коды, передаваемые финансовыми учреждениями на ваши мобильные устройства в виде смс-сообщений при подключении банковской карты к удаленным онлайн-сервисам;
- при осуществлении онлайн-оплат, заходить только на проверенные веб-сайты, сопоставлять наименование веб-сайта с официальным наименованием интернет-магазина либо поставщика финансовых услуг.
- никогда не переходить по ссылкам из писем, направленных в виде смс-сообщений, на электронную почту, в соцсети, мессенджерах;
- регулярно проводить тесты на наличие уязвимостей, чтобы четко знать точки проникновения в систему;
- использовать адекватные инструменты защиты, такие как файерволы и современные антивирусные решения;
- поддерживать персональный компьютер в обновленном состоянии. Это очень важно для повышения уровня безопасности системы, производительности и устранения ошибок в работе;

- не открывать файлы, вложения или ссылки из неизвестных и ненадежных писем, и не отвечать на такие письма;
- во избежание потерь данных периодически выполнять резервное копирование, особенно наиболее важной и чувствительной информации;
- остерегаться материалов экстремистского, террористического, порнографического характера, пропагандирующих культ насилия или жестокости. Они запрещены законодательством Республики Узбекистан.

Самое главное – необходимо помнить: даже при достижении максимального уровня технической защиты от посягательств киберпреступников, самым уязвимым звеном в этой системе всегда будет сам человек.

Список использованной литературы

1. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. No 1(1). С.2-9.
2. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности. М.: Изд-во КРАСАНД, 2011. 96 с.
3. Бородакий Ю.В., Боговик А.В., Карпов Е.А., Курносов В.И., Лободинский Ю.Г., Масановец В.В., Паращук И.Б. Основы теории управления в системах специального назначения. М.: Изд. Управление делами Президента Российской Федерации, 2008. 400 с.
4. Бородакий Ю.В., Лободинский Ю.Г. Эволюция информационных систем - М.: Горячая линия – Телеком, 2011. 368 с.
5. З. З. Кодиров, Д. В. Студенкова, Д. Ф. Косимов. “Возможности географических информационных систем в Узбекистане” - Молодой ученый учредители: ООО, 2022.
6. Inamova, G. A., & Kodirov, Z. Z. (2020). RELEVANCE AND DEVELOPMENT OF DISTANCE LEARNING IN UZBEKISTAN. Theoretical & Applied Science, (7), 60-62.

7. Кодиров, З. З., & Имамназаров, Э. Д. (2016). Применение электронных справочников в учебном процессе. Молодой ученый, (4), 154-155.
8. Кодиров, З. З., Ирискулов, Ф. С., Пулатов, А., & Умурзаков, Х. (2018). МОДУЛЬНОЕ ОБУЧЕНИЕ В СИСТЕМЕ ОБРАЗОВАНИЯ. Экономика и социум, (4 (47)), 381-386.
9. https://securelist.com/
10. infocom.uz