Кибербезопасность

Государственный комитет информационных технологий и связи КР

Национальная стратегия устойчивого развития

Построение цифровой Экономики

Реализация проекта – Умного города

На основе Знаний, Информации и Безопасности

Кибербезопасность

Определение Международного союза электросвязи (МСЭ)

Кибербезопасность — это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя.

Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде.

ATTACKS TODAY

(since 12AM PST)

26,767,561

ATTACKS YESTERDAY

39,194,695

- TOP TARGET COUNTRIES
- TOP ATTACKING COUNTRIES

TIME	ATTACK	ATTACKING COUNTRY	TARGET COUNTRY
09:25:15	Trojan.Win32.Injent.B	WA,USA	Netherlands
09:25:14	Trojan.Win32.Injent.B	WA,USA	Netherlands
09:25:14	Trojan.Win32.Injent.B	WA,USA	Netherlands
09:25:14	Trojan.Win32.Injent.B	WA,USA	Netherlands

Комплекс мероприятий

1 шаг	Анализ состояния	Концепция\ Стратегия кибербезопасности	**нормативно правовая база**
2 шаг	Оперативно-аналитический центр	Группа реагирования на компьютерные инциденты	Кибер-лаборатория
3 шаг	Международное сотрудничество	Повышение потенциала (HR)	Кибер-гигиена

Исследования состояния кибербезопасности страны

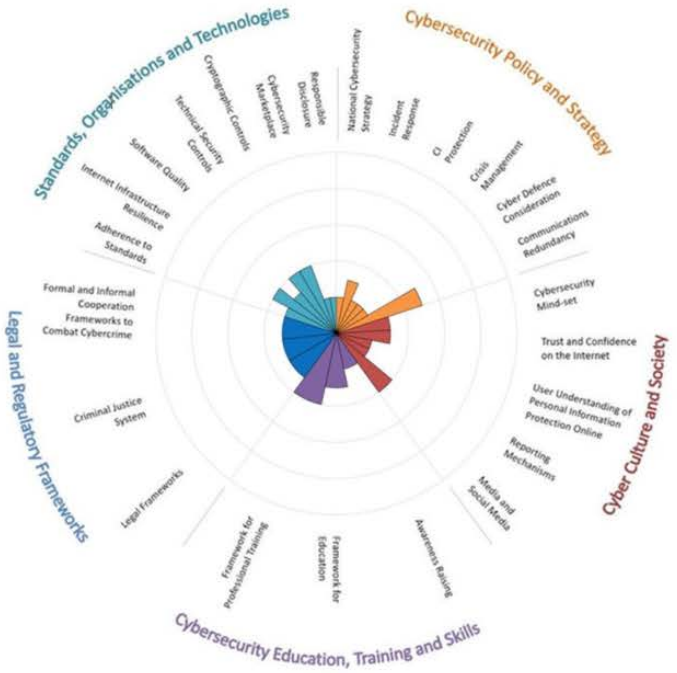
Проведены работы по оценке состояния развития кибербезопасности в Кыргызской Республике.

При содействии Всемирного Банка и Глобального центра развития потенциала в области кибербезопасности (Оксфордский университет, Великобритания) проведено страновой анализ Развития потенциала в области кибербезопасности Кыргызской Республики. По итогам работы подготовлен Отчет, в котором выработаны предложения по разработке политики и стратегии кибербезопасности в Кыргызской Республики.

WORLD BANK GROUP

Global
Cyber Security
Capacity Centre

Кибербезопасность: направление 1
Анализ состояния



5 параметров:

Параметр 1.

Политика и стратегия в области кибербезопасности

Параметр 2.

Культура и общество с точки зрения кибербезопасности

Параметр 3.

Образование,
обучение и навыки в области кибербезопасности

Параметр 4.

Законодательная и регулятивная база

Параметр 5.

Стандарты, организации и технологии

Разработка Стратегии кибербезопасности Кыргызской Республики

Целью настоящей Стратегии является обеспечение уровня кибербезопасности граждан, бизнеса и государства, позволяющего защитить их жизненно важные интересы в области использования ИКТ и обеспечить устойчивое социально-экономическое развитие Кыргызской Республики, включая цифровую трансформацию национальной экономики.

Задачи:

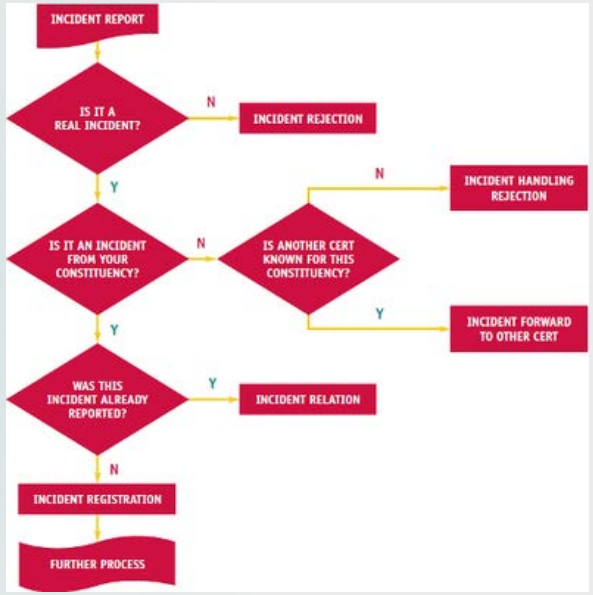
- Формирование единой системы мер обеспечения кибербзепасности;
- Противодействие компьютерной преступности;
- Формирование единого понятийного и методологического аппарата в области кибербезопасности и информационной безопасности;
- Обеспечение безопасности критической информационной инфраструктуры;
- Формирование национальной системы предупреждения, реагирования и управления компьютерными инциентами;
- Повышение уровня человеческих ресурсов и кадрового потенциала и т.д.

Уполномоченный орган по кибербезопасности

Основные возможности: **Оперативно аналитический центр (SOC):** командование и контроль

Обработка инцидентов

Что я делаю?



Осведомленность о ситуации

Что? Когда? Где?

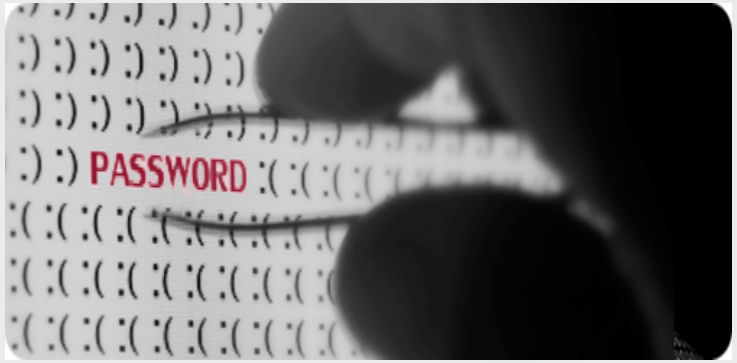
Основные возможности: **Группы реагирования на компьютерные инциденты:** предварительное оповещение

Анализ и мониторинг

Внутренний мониторинг

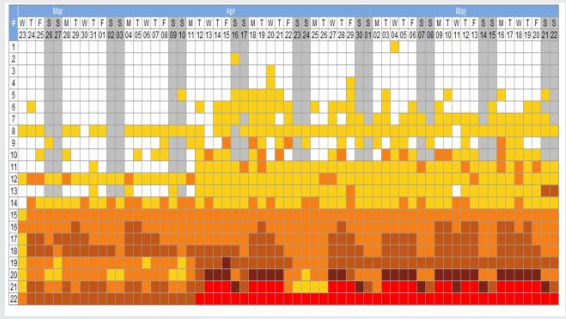
каналы и внешние источники

Уникальные источники



Основные возможности: **Кибер Лаборатории:** безопасность и аналитика

Анализ сети



Судебный анализ

Анализ вредоносных программ

Выездная команда

Основные возможности - **Учебного центра**

Повышение готовности

Создание тактических команд

Шаг 3.1.: Международное сотрудничество

Сотрудничество с Международным союзом электросвязи

ITU Global Cybersecurity Index

KOICA
Korea International Cooperation Agency

Сотрудничество со Всемирным банком

DCASA
KYRGYZ REPUBLIC

Deloitte.

KISA
Korea Internet & Security Agency

Повышение потенциала и кибер гигиена

- Ключевой задачей в части наращивания человеческого потенциала является внедрение систематизированного преподавания дисциплин кибербезопасности, компьютерной гигиены и грамотности в систему школьного, среднего профессионального и высшего образования КР. Для этой цели в горизонте 2020 г. Минобразования КР должно осуществить процесс пересмотра стандартов образовательной деятельности и образовательных регламентов, с целью включения:
- Дисциплины «кибербезопасность» в список профильных дисциплин для технических специальностей в высших образовательных учреждениях КР;
- Дисциплины «кибербезопасность» в список обязательных профильных дисциплин для технических специальностей в учреждениях среднего специального образования КР.
- Дисциплин «компьютерная гигиена» и «основы цифровой грамотности» в качестве обязательных предметов в учебных программах базового школьного образования КР.

Спасибо за внимание

Докладчик: главный специалист отдела Кибербезопасности ГКИТС Кыргызской Республики Абдылдаева Б.Б

Иссык-Куль 28-29 августа 2018 года