«КИБЕРЩИТ КАЗАХСТАНА»

ЧТО ХОТЕЛИ ПОСТРОИТЬ И ЧЕГО СМОГЛИ ДОСТИЧЬ.

Все большую актуальность приобретает борьба с киберпреступностью.

Поручаю Правительству и Комитету национальной безопасности принять меры по созданию системы «Киберщит Казахстана».

Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")

Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407

В целях реализации Указа Президента Республики Казахстан от 15 февраля 2017 года № 422 "О мерах по реализации Послания Главы государства народу Казахстана от 31 января 2017 года "Третья модернизация Казахстана: глобальная конкурентоспособность" Правительство Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую Концепцию кибербезопасности ("Киберщит Казахстана") (далее – Концепция).

2. Центральным государственным органам Республики Казахстан:

1) принять необходимые меры по реализации Концепции;

2) представлять раз в полугодие не позднее 10 числа месяца, следующего за отчетным полугодием, информацию в Министерство оборонной и аэрокосмической промышленности Республики Казахстан о ходе реализации Концепции.

3. Министерству оборонной и аэрокосмической промышленности Республики Казахстан:

1) в трехмесячный срок разработать План мероприятий по реализации Концепции и в установленном законодательством порядке внести на рассмотрение в Правительство Республики Казахстан;

2) представлять два раза год, к 25 июля и 25 января, сводную информацию о ходе реализации Концепции в Канцелярию Премьер-Министра Республики Казахстан.

4. Контроль за исполнением настоящего постановления возложить на Министерство оборонной и аэрокосмической промышленности Республики Казахстан.

5. Настоящее постановление вводится в действие со дня его подписания.

Премьер-Министр Республики Казахстан Б. Сагинтаев

Проведенное Международным союзом электросвязи исследование "Глобальный индекс кибербезопасности" (далее – Глобальный индекс кибербезопасности), оценивающее правовую, техническую, организационную готовность и потенциал 195 стран, зафиксировало 23 групповое место Казахстана с индексом 0,176 из 29 групп стран.

Ключевые проблемы

Ожидаемые результаты:

1) глобальный индекс кибербезопасности Казахстана к 2017 году составит 0,200, к 2018 году – 0,300, к 2019 году – 0,400, к 2020 году – 0,500, к 2021 году – 0,550, к 2022 году – 0,600;

2) повышение осведомленности об угрозах информационной безопасности к базовому периоду 2018 года в 2019 году – на 5%, в 2020 году – на 10%, в 2021 году – на 15%, в 2022 году – на 20%;

3) количество переподготовленных специалистов в сфере информационной безопасности в 2018 году – 300, в 2019 году – 500, в 2020 году – 600, в 2021 году – 700, в 2022 году – 800;

4) увеличение доли отечественных программных продуктов в сфере информатизации и связи, используемых в государственном и квазигосударственном секторах к базовому периоду 2017 года в 2018 году – на 10%, в 2019 году – на 20%, в 2020 году – 30%, в 2021 году – 40%, в 2022 году – 50%;

5) доля использования отечественных сертификатов безопасности при шифрованной передачи данных Интернет-ресурсами с доменом .KZ и .ҚАЗ в 2018 году составит 20%, в 2019 году – 40%, в 2020 году – 60%, в 2021 году – 80%, в 2022 году – 100%;

6) доля информационных систем государственных органов, негосударственных информационных систем, интегрируемых с государственными, информационных систем критически важных объектов информационно-коммуникационной инфраструктуры, подключенных к центрам мониторинга информационной безопасности, в 2018 году – 20%, в 2019 году – 40%, в 2020 году – 60%, в 2021 году – 80%, к 2022 году – 100%.

НАЧАЛЬНЫЕ УСЛОВИЯ И ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ

CIS

Member State	Score	Regional Rank	Global Rank
Russian Federation	0.836	1	26
Kazakhstan	0.778	2	40
Uzbekistan	0.666	3	52
Azerbaijan	0.653	4	55
Belarus	0.578	5	69
Armenia	0.495	6	79
Tajikistan	0.263	7	107
Kyrgyzstan	0.254	8	111
Turkmenistan	0.115	9	143

Table 6.5.1: Top three scores in the CIS region

Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
Russian Federation	0.836	0.197	0.162	0.177	0.166	0.135
Kazakhstan	0.778	0.179	0.143	0.174	0.160	0.122
Uzbekistan	0.666	0.123	0.142	0.112	0.143	0.144

Сноска. Глава 2 дополнена статьей 7-2 в соответствии с Законом РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти кале после дня его первого официального опубликования).

Статья 7-3. Служба реагирования на инциденты информационной безопасности

1. Служба реагирования на инциденты информационной безопасности:

1) проводит анализ информации о событиях информационной безопасности в целях устранения причин и условий инцидентов информационной бе

2) вырабатывает рекомендации, направленные на противодействие угрозам информационной безопасности;

3) информирует владельцев объектов информатизации о ставших известными инцидентах и угрозах информационной безопасности.

2. Служба реагирования на инциденты информационной безопасности осуществляет свою деятельность на основании лицензии на оказание услу технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий.

3. Сотрудники службы реагирования на инциденты информационной безопасности несут ответственность за разглашение коммерческой или иной законом тайны, полученной ими в результате своей деятельности, в соответствии с законами Республики Казахстан.

4. Требование пункта 2 настоящей статьи не распространяется на банки второго уровня Республики Казахстан, в которых функции службы реаги инциденты информационной безопасности осуществляются их структурными подразделениями.

ИЗМЕНЕНИЯ В ЗАКОНЕ ОБ ИНФОРМАТИЗАЦИИ

Сноска. Глава 2 дополнена статьей 7-1 в соответствии с Законом РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 7-2. Оперативный центр информационной безопасности

1. Оперативный центр информационной безопасности:

1) осуществляет деятельность по обнаружению, оценке, прогнозированию, локализации, нейтрализации и профилактике угроз информационной безопасности информационно-коммуникационной инфраструктуры, объектов информатизации, подключенных к оперативному центру информационной безопасности;

2) принимает меры по минимизации угроз информационной безопасности, незамедлительно информирует владельца информационно-коммуникационной инфраструктуры, а также Национальный координационный центр информационной безопасности о факте инцидента информационной безопасности;

3) осуществляет мониторинг обеспечения информационной безопасности по выявлению, пресечению и расследованию угроз информационной безопасности информационно-коммуникационной инфраструктуры, объектов информатизации, подключенных к оперативному центру информационной безопасности;

4) осуществляет обмен информацией, необходимой для обеспечения информационной безопасности объектов информатизации, подключенных к оперативному центру информационной безопасности, с Национальным координационным центром информационной безопасности и другими оперативными центрами информационной безопасности;

5) осуществляет сбор, консолидацию, анализ и хранение сведений о событиях и инцидентах информационной безопасности;

6) предоставляет владельцам критически важных объектов информационно-коммуникационной инфраструктуры информацию, необходимую для обеспечения информационной безопасности объектов информационно-коммуникационной инфраструктуры, в том числе информацию об угрозах безопасности, уязвимости программного обеспечения, оборудования и технологий, способах реализации угроз информационной безопасности, предпосылках возникновения инцидентов информационной безопасности, а также методах их предупреждения и ликвидации последствий;

7) обеспечивает сохранность сведений ограниченного распространения, ставших известными оперативному центру информационной безопасности в рамках осуществления его деятельности;

8) обеспечивает подключение систем журналирования событий информационной безопасности к центру мониторинга Национального координационного центра информационной безопасности.

2. Оперативный центр информационной безопасности осуществляет свою деятельность на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий.

3. Сотрудники оперативного центра информационной безопасности несут ответственность за разглашение коммерческой или иной охраняемой законом тайны, полученной ими в результате своей деятельности, в соответствии с законами Республики Казахстан.

4. Требование пункта 2 настоящей статьи не распространяется на банки второго уровня Республики Казахстан, в которых функции оперативного центра

На оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

- Специалист с высшим или средне профессиональным техническим образованием
- Наличие поисковых технических средств согласно приложению
- Оценка уровня знаний заявленных лиц (зачет). Вопросы по разработке, производству, ремонту СТС.
- Выделенное помещение с металлическими решетками на окнах, системами охранной и пожарной сигнализации …
- Наличие методики проведения работ по выявлению технических каналов утечки информации и СТС, оценки эффективности защищенности помещений от утечки информации по техническим каналам; журнал учета заключенных договоров …

ЗАДАЧА – РОСТ МЕСТНОЙ КВАЛИФИКАЦИИ

CEH CHFI OSCP OSWP OSCE OSEE OSWE

CISO CISSP CISA CISM

RHCE RHCSA RHCSS

ISO 27001

…

РЕЕСТР ДОВЕРЕННОЙ ПРОДУКЦИИ ЭЛЕКТРОННОЙ ПРОМЫШЛЕННОСТИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

13	02.04.2019 г.	Программное обеспечение «Система мониторинга событий информационной безопасности «MAxPatrol SIEM CA»	-	Программное обеспечение предназначено для обеспечения комплексного контроля защищенности, мониторинга и корреляции событий информационной безопасности.	262021	8471709800	2620	ТОО «Позитивные технологии»	-	Договор об отчуждении исключительных прав на объекты исключительного права-программы для ЭВМ № 01-04/2018 от 06.04.2018 г.	Приказ и.о. Министра цифрового развития, оборонной и аэрокосмической промышленности № 24/НҚ от 3 апреля 2019 г.	-	№ KZ.7500633.05.01.00014 от 01.10.2018 г., ОПС ТОО «Инфосерт»


ПРОЦЕССЫ
ЧЕЛОВЕЧЕСКИЙ ФАКТОР
ТЕХНОЛОГИЯ

НКЦИБ

ОЦИБ ОЦИБ ОЦИБ

КВОИКИ КВОИКИ КВОИКИ КВОИКИ

СУЩЕСТВУЮЩИЕ ОЦИБ

ЦАРКА
ЦЕНТР АНАЛИЗА
И РАССЛЕДОВАНИЯ
КИБЕР АТАК

Tengri
Security

NITEC

TTC
Transtelecom

Информационно-коммуникационная инфраструктура Республики Казахстан

Критически важные объекты ИКИ - **219**

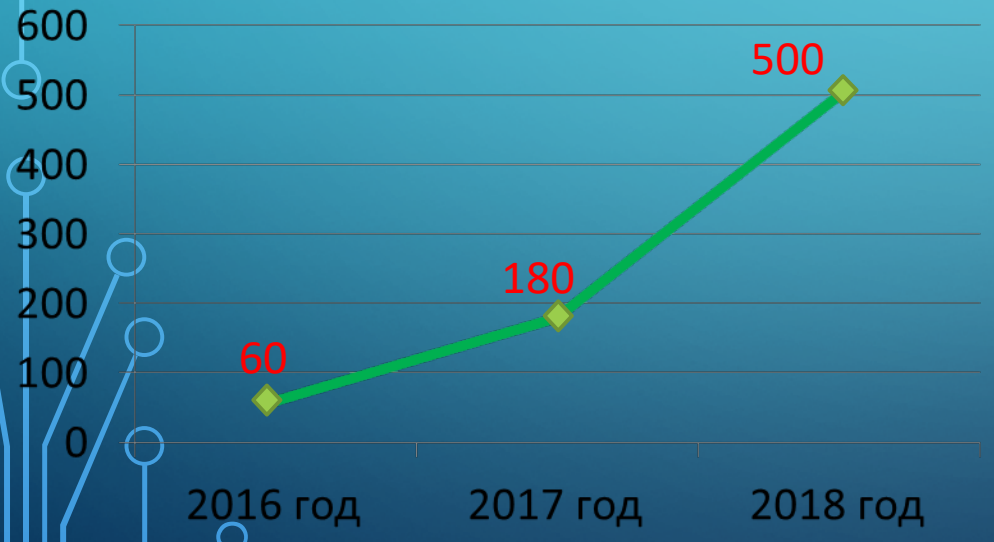
- Государственные услуги - **79**
- Транспорт - **49**
- Космическая сфера - **6**
- Инфраструктура - **45**
- Нефтегазовая сфера - **14**
- В сфере энергетики - **24**
- Металлургическая сфера - **2**

Усиление потенциала

В государственных органах стало обязательным наличие выделенного подразделения по информационной безопасности – **численность занятых работников составляет 1400.**

МОАП совместно с Академией государственного управления обеспечена ежегодная подготовка и переподготовка **более 200 государственных служащих.**

Гранты ВУЗов



Общая емкость рынка труда составляет **35000 человек** различных уровней квалификации и специализации.

Разработаны **5 профессиональных стандартов** в сфере информационной безопасности.

ВНТК одобрено 12 проектов НИОКР по направлению информационной безопасности.


The End