АКАДЕМИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ КАЗАХСТАН

Институт дипломатии

на правах рукописи

Жакибеков Ержан Тукенович

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В СФЕРЕ КИБЕР-БЕЗОПАСНОСТИ

Образовательная программа «7М03111 - Международные отношения»
по направлению подготовки «7М031 Социальные науки»

Магистерский проект на соискание степени
магистра международных отношении

Научный руководитель: Сомжурек Баубек Жұмашұлы,
кандидат исторических наук,
ассоциированный профессор

Проект допущен к защите: «10» июня 2022 г.

Директор Института дипломатии: Абишева Мариан Асаровна,
кандидат политических наук, (Phd)

Нур-Султан, 2022

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ 3
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ. 4
ВВЕДЕНИЕ 5
ОБЗОР ЛИТЕРАТУРЫ 6
МЕТОДЫ ИССЛЕДОВАНИЯ 8
ГЛАВА 1. КОНЦЕПТУАЛЬНЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ В МИРЕ В КОНТЕКСТЕ ГЛОБАЛЬНЫХ УГРОЗ
1.1 История защиты информации 9
1.2 Теоретико-правовые аспекты кибербезопасности 17
1.3 Современные угрозы кибербезопасности 25
ГЛАВА 2. О ДЕЙСТВУЮЩЕЙ СИСТЕМЕ КИБЕРБЕЗОПАСНОСТИ И ПОТЕНЦИАЛЬНЫХ УГРОЗА В РЕСПУБЛИКЕ КАЗАХСТАН
2.1 Система обеспечения кибербезопасности в Казахстане 28
2.2 Новые вызовы для безопасности Республики Казахстан в киберпространстве 34
ЗАКЛЮЧЕНИЕ 38
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 41
ПРИЛОЖЕНИЯ 44

НОРМАТИВНЫЕ ССЫЛКИ

Нормативные ссылки, используемые в проекте:

1. Закон Республики Казахстан «О национальной безопасности Республики Казахстан» № 527-IV от 06.01.2012 года (с изменениями и дополнениями по состоянию на 27.12.2021 г.);
2. Закон Республики Казахстан «О ратификации Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» №286-IV от 01.06.2010 года;
3. Закон Республики Казахстан «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» от № 277-VI от 09.12.2019 года;
4. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации»;
5. Уголовный кодекс Республики Казахстан № 226-V от 03.07.2014 года;
6. Уголовно-процессуальный кодекс Республики Казахстан от от 4 июля 2014 года № 231-V ЗРК;
7. Кодекс Республики Казахстан об административных правонарушениях № 235-V 05.07.2014 года;
8. Постановление Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» № 832 от 10.12.2016 года;
9. Постановление Правительства Республики Казахстан «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")» № 407 от 30.06.2017 года;
10. Постановление Правительства Республики Казахстан от 28 октября 2004 года № 1118 «Вопросы Министерства иностранных дел Республики Казахстан»;
11. Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827 «Об утверждении Государственной программы "Цифровой Казахстан"»;
12. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры»;
13. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 31 января 2018 года № 21/НҚ «Об образовании совета по обеспечению информационной безопасности»;
14. Конвенция о киберпреступлениях, Будапешт, 23/11/2001 г. (Convention on Cybercrime CETS № 185).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ГА	-	Генеральная Ассамблея
ГИК	-	Глобальный индекс кибербезопасности
ГП	-	Генеральная прокуратура
ГПЭ	-	Группы правительственных экспертов
ГТС	-	Государственная техническая служба
ЕС	-	Европейский союз
ОДКБ	-	Организация Договора о коллективной безопасности
ООН	-	Организация объединенных наций
МВД	-	Министерство внутренних дел
МИД	-	Министерство иностранных дел
МЦРиАП	-	Министерство цифрового развития и аэрокосмической промышленности
МСЭ	-	Международный Союз Электросвязи
НАТО	-	Организация Североатлантического договора, Североатлантический Альянс (North Atlantic Treaty Organization)
НПО	-	неправительственные организации
ОЭСР	-	Организации экономического сотрудничества и развития
ОЮЛ	-	Объединение юридических лиц
ПЦР	-	Полимеразная цепная реакция
ПО	-	Программное обеспечение
РК	-	Республика Казахстан
РФ	-	Российская Федерация
СНГ	-	Содружество Независимых Государств
США	-	Соединенные Штаты Америки
УК	-	Уголовный кодекс
УПК	-	Уголовно-процессуальный кодекс
ИКТ	-	Информационно-коммуникационные технологии
ЦА	-	Центральная Азия
ЦАРКА	-	Центр анализа и расследования кибератак
ФРГ	-	Федеративная Республика Германия
ШОС	-	Шанхайская организация сотрудничества
ЭВМ	-	Электронно-вычислительная машина
GCSCC	-	Global Cyber Security Capacity Centre
MIT	-	Massachusetts Institute of Technology
DoS	-	Denial of Service «отказ в обслуживании»
CERT	-	Computer emergency response team
RIA	-	Riigi Infosüsteemi Amet (Департамент государственной инфосистемы)
PEST	-	Political, economic, social, technology s
SWOT	-	Strong, weak, opportunities, threats

ВВЕДЕНИЕ

В последние десятилетия во всем мире существует устойчивая тенденция внедрения технологических инноваций в общественные отношения, при этом культура их пользования значительно отстает от самого прогресса, что порождает не менее инновационные риски и угрозы не только для общества, но и для государств, в связи с чем аспекты информационной безопасности выходят на более приоритетный уровень в обеспечении национальной безопасности.

Еще в 2019 году Президент Республики Казахстан К-К. Токаев на заседании Совета глав государств – членов Шанхайской организации сотрудничества акцентировал особое внимание на нарастающих угрозах в киберпространстве. Глава государства обозначил, что проблема терроризма приобретает новые очертания и в современном мире активно применяет информационные технологии, что в свою очередь требует особого внимания вопросам кибербезопасности [1].

Кибербезопасность стала серьезной проблемой не только коммерческого и частного характера, а создало реальную угрозу безопасности любого государства без исключения. Ежедневно фиксируется более 40 млн. кибератак по всему миру [2]. Новые технологи настолько тесно интегрированы в гражданское общество, торговлю, управление, критическую инфраструктуру, сбор разведданных и правоохранительные органы, что заинтересованные стороны, необходимые для практики и политики кибербезопасности, разнообразны и сложны. Это приводит к столкновению интересов, программ и ожиданий, которые часто могут быть несовместимыми или даже прямо противоречить друг другу. И, конечно же, некоторые аспекты технологий могут быть совершенно независимыми от географических и политических границ.

В конце 90-х, когда было принято постановление Правительства Республики Казахстан от 31 декабря 1998 года № 1384 «О координации работ по формированию и развитию национальной информационной инфраструктуры, процессов информатизации и обеспечению информационной безопасности», было принято 3 новых редакции законов Республики Казахстан «Об информатизации» и несколько специализированных законов.

Несмотря на то, что кибербезопасность является «постгосударственной» проблемой, на самом деле оказалось очень трудно выйти за рамки Вестфальской концепции. Это приводит к ключевому парадоксу кибербезопасности в том виде, в котором она находится в настоящее время. С одной стороны, кажется, что это проблема, с которой не могут эффективно справиться государственные инструменты, такие как вооруженные силы или правоохранительные органы, но, несмотря на это, остаются большие надежды, что государство сохраняет за собой ответственность за обеспечение безопасности в этой сфере. Этот парадокс привел к акценту в бесконечных переговорах по разработке различных документов по вопросам международной кибербезопасности.

С момента запуска программы «Цифровой Казахстан» процессы диджитализации в Казахстане значительно расширили свое применение в

государственном и частном секторах.

Учитывая, что сфера информатизации, в том числе вытекающие из нее возможности и риски не ограничиваются государственными границами или конкретными правилами, для ее регулирования необходима конструктивное участие всех участников этого глобального процесса.

Таким образом, актуальность вопросов обеспечения информационной безопасности Казахстана, необходимость международной интеграции, дальнейшее теоретическое и практическое развития сферы определили выбор темы исследования.

Нормативно-правовую базу исследования составляют как международные договоры, конвенции и резолюции, так и национальные нормативно-правовые акты, регулирующие вопросы обеспечения информационной безопасности и деятельность правоохранительных органов.

Объектом исследования являются общественные отношения, которые регламентируются нормами международного права в сфере глобального партнерства стран/коалиций/союзов в области обеспечения кибербезопасности.

Предмет исследования включает нормативно-правовые акты регламентирующие процессы взаимодействия заинтересованных сторон, в том числе правительства стран, международные не правительственные и коммерческие организации в области развития глобальной системы кибербезопасности.

Цель магистерского проекта является проведение анализа всех аспектов международного сотрудничества, направленного на укрепление и развитие взаимоотношений между странами комплексный анализ вопросов международного сотрудничества государств в сфере информационной безопасности.

Задачи:

1) определить характера разногласий используемых в мире терминологий и понятий по вопросам кибербезопасности;
2) выявить потенциальные риски, связанные с кибернетическими атаками для межправительственного сотрудничества;
3) рассмотреть нормативно-правовую базу, регламентирующую деятельность по обеспечению кибербезопасности;
4) проанализировать текущее состояние системы кибербезопасности в Республике Казахстан;

Методологическая основа работы. В данной работе применялись специальные методы: контент-анализ, кейс-анализ, PEST-анализ, SWOT-анализ и обработка статистических данных.

Структура работы включает в себя введение, две главы, заключение и список использованной литературы.

Практическая значимость. Результаты исследования могут быть использованы государственными органами при разработке мер и мероприятий по подготовке стратегии информационной безопасности Казахстана.

ОБЗОР ЛИТЕРАТУРЫ

Для определения понятийного аппарата исследования были изучены научные работы ученных ближнего и дальнего зарубежья, а также национальное законодательство.

Ученные Нижегородского Государственного университета им.Лобачевского описывают «Информационную безопасность как невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз)» [3].

В соответствии с глоссарием терминов по информационной безопасности Национального института стандартов и технологий Департамента коммерции США, составленный г-ном Ричардом Кисселем, информационная безопасность — это защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения с целью обеспечения конфиденциальности, целостности и доступности [4];

При изучении данного вопроса необходимо четко различать понятия информационная и кибербезопасность. Козлова Н.Ш. и Довгаль В.А., в своей научной статье «Кибербезопасность и информационная безопасность: сходства и отличия» дали более чем развернутое объяснение этим понятиям. Основная суть заключается в разнице защищаемого предмета. Так, по мнению ученных, «кибербезопасность – это область информационных технологий, ориентированная на защиту систем, включающих в себя электронные записи, устройства для отслеживания информации, оборудование и программное обеспечение, используемое для оказания услуг и управления ими», а информационная безопасность имеет более широкое понятие [5].

Эксперты технологической консалтинговой компании «TechTarget» Шэрон Ш., Александр С. Джиллис и Кейси Кларк в своей статье «Что такое кибербезопасность?» дают простое однозначное определение, кибербезопасность — это защита подключенных к Интернету систем, таких как оборудование, программное обеспечение и данные, от киберугроз [6].

В национальном законодательстве Республики Казахстан применяется понятие информационная безопасность. Так, в соответствии с Законом «О национальной безопасности», Касательно применения понятия в отечественном законодательстве, «информационная безопасность – состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны» [7].

В ходе исследования применяются оба понятия информационной и кибербезопасности, исходя из контента излогаемой ситуации.

МЕТОДЫ ИССЛЕДОВАНИЯ

При написании данного магистерского проекта использованы методологические принципы, которые позволяют объективно исследовать проблематику международного сотрудничества в сфере кибер-безопасности, а также исходящие из этого риски дя Республики Казахстан.

В качестве общенаучных использованы метод синтеза и метод экспертной оценки, которые позволили определить понятия кибербезопасности и информационной безопасности, их приминение и понимания экспертами ближнего и дальнего зарубежья, а также в Республики Казахстан, синтезировать собственное представление термина и определить его содержание.

В аналитической части исследования использованы методы сравнительного анализа, кейс-анализа, PEST и SWOT анализы в контексте основных положений и концепций теории международных отношений.

Применение PEST – анализа позволило определить масштабы и потенциальные последствия для Казахстана от наступления киберугроз в политических, экономических, социальной и технологической сферах.

Благодаря SWOT – анализу удалось предварительно определить успешность реализации Концепции «Киберщит», ее слабые и сильные стороны, а также будущие возможности для ее реализации.

В результате применения вышеназванных методов исследования осуществлено обобщение материалов, выработка рекомендаций и ключевых моментов на которые в будущем следует обратить внимание.

1 КОНЦЕПТУАЛЬНЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ В МИРЕ В КОНТЕКСТЕ ГЛОБАЛЬНЫХ УГРОЗ

1.1 История защиты информации и кибербезопасности

Защита информации с древних времен являлась важным аспектом управления государством. Правители управляли народом, заключали союзы, вели переговоры и военные действия, опираясь на коммуникации, защищенные от внимания недоброжелателей. Последствия раскрытия секретной информации могли послужить проигрышем битвы или даже крахом целого государства.

Впервые о секретных записках говорилось в работах Геродота, великого историка Древней Греции. В своих работах он описывал конфликт между правителем Персии Ксерксом и царём Греции Леонидом I. Об этих событиях в Голливуде снят фильм «300 спартанцев», а также вторая часть этого фильма. В записях Геродота говорится, правитель персов, на протяжении 5 лет, тайно готовил самую огромную армию того времени, для вторжения в Грецию [8].

Об этом узнал грек по имени Демарт, который проживал в одном из персидских городов. Но сообщить об этом он не мог, так как был большой риск перехвата сообщения солдатами Ксеркса. Тогда Демарт придумал хитрый план, который заключался в тайном послании правителю греков. Проблема заключалась в том, что на границе все проверялось солдатами персов. В те времена для письма использовались деревяшки, покрытые воском. Как раз такие и использовал Демарт, но перед этим он очистил их от воска, а свое послание с описанием планов вторжения Ксеркса он написал на дереве и спрятал под толстым слоем нового воска. Тайное сообщение успешно прошло все границы и попало в руки царя Леонида I, царя Лаконики в 491-480 гг.до н.э. Однако, никто не мог понять зачем некий Демарт передал царю пустое сообщение и только жена Леонида I Горго догадалась о соскоблить дощечки от воска [8].

Сообщение было расшифровано, другие города Греции были незамедлительно предупреждены, все силы были брошены на военное производство, армию и флот. Ксеркс утерял элемент внезапности, 23 сентября 480 г. до н.э., его корабли достигли Саламинского пролива, в котором он ожидал настичь слабых греков врасплох, вместо этого он столкнулся с мощной, боеспособной армией Греков. В течение одного дня огромные силы персов были уничтожены. Вот так, одно маленькое зашифрованное сообщение спасло целое государство [8].

В современном мире киберпреступления принято относить ко времени появления интернета. Однако многие не знают, что Интернет и кибербезопасность были факторами задолго до этого. Сегодня компании часто работают над тем, чтобы свести к минимуму кибератаки, чтобы обеспечить безопасность потребительских и коммерческих данных, информации с высокой степенью риска и многого другого. Для этого им необходимо заниматься вопросами кибербезопасности.

Понимание истории кибербезопасности может пролить свет на то, насколько она глубока и насколько важны люди для предотвращения

возникновения этих рисков.

Киберпреступность значительно изменилась с тех пор, как первые компьютеры вышли в сеть и начали общаться друг с другом. Уровень риска, с которым сталкиваются сегодня, значительно выше, чем во второй половине XX века, но кибер угрозы, всегда беспокоили пользователей компьютеров, и не без оснований.

По мере совершенствования технологий могут развиваться и киберугрозы. Преступники в отрасли часто продолжают разрабатывать новые способы проникновения и сбора информации. Они могут использовать вредоносное программное обеспечение (ПО) и программы-вымогатели, чтобы вывести из строя все, от мясокомбинатов до топливопроводов, проходящих через всю страну.

Многие могут подумать, что киберпреступность началась в последние несколько десятилетий. Тем не менее, компьютерные системы страдали от уязвимостей гораздо раньше. Киберпреступники уже давно занимаются противоправной деятельностью. Факторы, влияющие на развитие этой отрасли со времен Второй Мировой войны.

Первый цифровой компьютер был создан в 1943 году. В течение следующих нескольких десятилетий у людей было ограниченное количество способов использования компьютеров преступным или рискованным образом. В мире было всего несколько таких компьютеров. Большинство из них были очень большими, очень шумными и сложными в использовании. Эти электронные машины были недоступны большинству людей. Многие не знали, что они существуют [9].

Более того, в 1940-х годах не было и соединительной сети. Между компьютерами не было связи для перемещения данных или файлов. Это создало, можно сказать, безопасный климат. Угроз почти не было [9].

Однако в конце десятилетия разработана теория о вирусах. Джон фон Нейман считал, что может возникнуть некий тип «механического организма», что могло повредить машины. Механический организм может копировать себя, как естественный вирус. И это может распространиться и на новых «хозяев». Нейман разработал эту теорию и написал о ней в статье «Теория самовоспроизводящихся автоматов», которую он опубликовал позже в 1966 году [10].

Хакерство изначально не разрабатывалось как способ сбора информации с помощью компьютеров. Скорее, корни компьютерного хакерства могут быть более эффективно связаны с ранним использованием телефона. Это очевидно в 1950-х годах, когда началась тенденция, называемая телефонным фрикингом [11].

Телефонные фрики — это люди, которые проявляли значительный интерес к тому, как работают телефоны. Они попытались захватить существующие протоколы, которые позволили инженерам работать в сети на расстоянии. Это позволило людям совершать бесплатные звонки и снизить плату за междугородние звонки. Эта практика продолжалась некоторое время. Это

оставило многие телефонные компании без возможности предотвратить это [11].

Есть утверждения, что Стив Джобс и Стив Возняк, основатели Apple, интересовались самим сообществом телефонных фриков. Цифровые технологии, использующие аналогичные концепции, позже будут разработаны в компьютерах Apple [11].

1960-е годы принесли с собой различные инновации в компьютерной индустрии. Тем не менее, компьютеры все еще были очень большими и дорогими системами. Большинство из них представляли собой огромные мейнфреймы, которые при использовании были заперты в комнатах вдали от доступа широкой публики или кого-либо еще, кто их использовал [12].

По большей части термин «взлом» появился в течение этого десятилетия. Это произошло не из-за использования компьютеров, а, скорее, когда группа людей из студенческой организации Массачусетского технологического института Tech Model Railroad Club взломала высокотехнологичные поезда. Они хотели внести коррективы в их функциональность. Та же самая предпосылка сделала переход к компьютерам в этом году [12].

Тем не менее взлом и получение доступа к этим ранним компьютерам не казались каким-то открытием. Фактически, эти ранние хакерские атаки были просто направлены на получение доступа к системам. Однако никаких политических или коммерческих выгод от этого не могло быть. Скорее, ранний взлом был больше связан с созданием проблем, чтобы увидеть, можно ли это сделать.

Со временем появились новые, более быстрые и эффективные способы взлома. Одно ключевое событие произошло в 1967 году. В то время IBM пригласила группу студентов в свои офисы, чтобы опробовать недавно разработанный компьютер. Студенты узнали о языке компьютерной системы. Они получили доступ к различным частям системы. Это дало IBM представление об уязвимостях системы [13].

Результатом стало развитие защитного мышления, согласно которому компьютеры требовали мер безопасности для защиты от хакеров. Возможно, это был первый пример белого хакерства в отрасли.

Это был важный шаг в разработке стратегий кибербезопасности. Во второй половине этого десятилетия, а тем более в последующие годы, компьютеры стали использоваться более активно. Они также стали меньше в размерах. Это означало, что компании могли себе их позволить. Многие организации так и поступили, купив технологию как способ хранения данных. Как они это делали, запирать компьютеры в комнате казалось невыполнимым или не выгодным. Слишком много сотрудников нуждались в доступе к работе на этих компьютерах. Вот тогда и зародилось использование паролей для доступа к компьютеру [14].

Настоящее рождение кибербезопасности произошло в 1970-х годах. Это началось с проекта под названием The Advanced Research Projects Agency Network (ARPANET). Это была сеть подключения, разработанная до появления самого Интернета [15].

Боб Томас определил, что компьютерная программа может перемещаться по сети. При этом программа оставляла след во время своего движения. Он разработал программу так, чтобы она могла перемещаться между терминалами Tenex в сети ARPANET [15].

Б. Томас назвал эту программу Creeper, для переноса и печати простого сообщения. «Я крипер: поймай меня, если сможешь» [16].

Это вызвало большой интерес и некоторое беспокойство. Именно это сообщение подтолкнуло Рэй Томлинсон к разработке новой программы. Он назвал эту программу Reaper. Р. Томлинсон, прославившийся разработкой электронной почты, разработал Reaper, чтобы преследовать и удалять Creeper [16].

Reaper — это первый пример антивирусной программы. Ее также называли самовоспроизводящейся программой. Это сделало Reaper первым в мире компьютерным червем [16].

В это время компьютерные технологии продолжали расти и расширяться. Большинство сетей полагались на телефонные системы для связи. Это поставило новый, более высокий уровень требований к способам защиты сетей. Каждое устройство, подключенное к сети, создавало новый тип точки входа. Это были уязвимости в сети.

В этот момент разработка решений в области безопасности была еще более важной. Правительства начали обсуждать способы уменьшения этих уязвимостей. Правительства узнали, что несанкционированный доступ к этой большой системе может создать множество проблем. Во второй половине десятилетия был написан ряд научных работ, посвященных изучению способов обеспечения такой безопасности. Они также подробно рассказали об ожидаемых рисках.

Подразделение электронных систем (Eelectronic System Department) командования военно-воздушных сил США начало работу над проектами. Агентство перспективных исследовательских проектов также принимало участие. Это было подразделение Министерства обороны США. Их задачей была разработка системы безопасности для ранней операционной системы Honeywell Multics [13].

Другие организации также начали работать над сетевой безопасностью. Сюда входят Стэнфордский исследовательский институт и Калифорнийский университет в Лос-Анджелесе.

Проект анализа защиты от ARPA был ключевым компонентом разработки. Он рассматривал широкий спектр тем. Это включает в себя выявление уязвимостей. Он работал над различными аспектами безопасности операционной системы. Он также стремился разработать автоматизированные методы обнаружения уязвимостей в программах. Все это были новые темы и идеи в отрасли [13].

К середине десятилетия развитие кибербезопасности развивалось быстрыми темпами. Теперь разработчикам компьютеров необходимо было также сосредоточиться на создании безопасных и защищенных систем.

В 1979 году, когда десятилетие подходило к концу, был арестован первый киберпреступник. Его звали Кевин Митник. Ему было всего 16 лет. Ему удалось взломать систему телефонных связей «Ковчег». Ковчег был массивной системой, которая использовалась для разработки операционных систем. К. Митнику удалось сделать копии программного обеспечения после того, как он получил к нему доступ. Он был схвачен за свои действия, арестован и заключен в тюрьму в связи с этими действиями. Это стало началом многочисленных кибератак, произошедших в ближайшие десятилетия [17].

С появлением современных кибератак это десятилетие принесло множество проблем для компьютерных сетей. В этом десятилетии произойдет ряд громких атак. Сюда входят атаки на американский транснациональный телекоммуникационный конгломерат «AT&T», Лос-Аламосскую национальную лабораторию и Национальную систему обслуживания клиентов. В 1983 году были разработаны новые термины для описания этих атак. Среди них были «компьютерный вирус» и «троянский конь» [13].

Большим страхом в это время была угроза со стороны других правительств. Это была середина холодной войны. Страх кибершпионажа был вполне реальным. Это подтолкнуло правительство США к созданию новых руководств и ресурсов для управления такими событиями и угрозами. Критерии оценки надежных компьютерных систем были разработаны в 1985 году Министерством обороны США. Позже она была названа «Оранжевой книгой» [18].

Это руководство было ценным, поскольку оно было одним из первых руководств по безопасности компьютеров. Его целью было оценить, насколько доверяют программному обеспечению, использующему любой тип конфиденциальной информации. Он также установил некоторые основные меры безопасности, которые необходимо учитывать при производстве программного обеспечения. Это создаст основу для разработки коммерческих компьютерных программ с точки зрения кибербезопасности [18].

Угроза была реальной. Маркусу Хесс, хакеру из Германии, удалось проникнуть в правительственные системы в 1986 году. Он использовал интернет-шлюз, расположенный в Калифорнии. Для этого он подключился к ARPANET. Результат был поразительным. За считанные минуты Хесс смог получить доступ примерно к 400 военным компьютерам. Среди них были мэйнфреймы, используемые самим Пентагоном. Он планировал продать всю собранную информацию Комитету государственной безопасности СССР [19].

Атака заставила многие компании задуматься, что делать. С этого момента безопасности стало уделяться больше внимания. Информация и стратегии по снижению таких рисков были быстро разработаны. Например, одной большой тенденцией была необходимость отслеживать размер отправляемых файлов. Чем больше был файл, тем больше вероятность того, что он содержит вирус или другую опасность.

Еще одним признаком было уменьшение оперативной памяти. Если это произойдет, это может сигнализировать о заражении компьютерной системы.

Сегодня замедление работы компьютера по-прежнему является признаком возможной вредоносной активности.

В конце этого десятилетия началось развитие индустрии кибербезопасности. Коммерческие антивирусные продукты были впервые разработаны и выпущены в 1987 году, всего через год после атаки Пентагона [13].

До сих пор ведутся споры о том, кто разработал первый антивирус. Среди наиболее известных VirusScan, продукта, разработанного Джоном Макафи, который впоследствии основал свою собственную компанию с таким же названием и антивирусное решение NOD, которое было выпущено в Чехословакии [20].

Это также был год вируса Cascade. Это был один из первых зашифрованных вирусов. Он перемещался и заражал файлы .com. Хотя сам вирус был очень вредоносным, например, Cascade удалось заразить компьютерные системы IBM. Важно упомянуть о нем еще и потому, что он стимулировал разработку новых антивирусных решений [20].

Развитие компьютерного червя также процветало в 1980-х годах. Некоторые говорят, что его разработал Роберт Т. Моррис. Он был студентом Корнуэллского университета и хотел определить размер Интернета в целом. Для этого в 1988 году он создал червя. Целью червя было проникновение и заражение UNIX-систем. При заражении он будет подсчитывать соединения, присутствующие в Интернете. Это тоже был самовоспроизводящийся вирус [21].

План мистера Морриса не сработал. Ошибка в дизайне программы привела к тому, что она заражала каждую машину одну за другой. Это привело к тому, что сети были забиты информацией, что привело к массовым сбоям. Программа была агрессивной и в итоге сделала интернет медленным. Это было одним из первых широко освещаемых событий в области кибербезопасности [21].

Этот червь был уникален и в том, как он был написан. Он был первым, кто использовал уязвимости системы. Г-н Моррис был также первым человеком, которому было предъявлено обвинение в соответствии с Законом о компьютерном мошенничестве и злоупотреблениях. Разработанный им червь привел к созданию группы реагирования на компьютерные чрезвычайные ситуации [21].

Это событие также вызвало изменения в самой кибербезопасности. Теперь все больше людей искали способы создания более смертоносных и эффективных червей и вирусов. Чем больше у людей возникали эти проблемы, тем больше они развивались и становились более инвазивными. Чтобы противодействовать этому, возрастала потребность в разработке новых антивирусных решений, которые могли бы быстро реагировать на эти проблемы.

К концу десятилетия на рынке появилось множество антивирусных решений. Сюда входят Norman Virus Control, ThunderBYTE и F-Prot. IBM также выпустила для широкой публики свой ранее использовавшийся внутри компании продукт. Это было одно из первых решений IBM VirusScan и MS-DOS [20].

Целое десятилетие было отмечено невероятным ростом и развитием Интернета. Индустрия кибербезопасности росла вместе с ней. Вот некоторые ключевые события.

Разработаны полиморфные вирусные риски. В 1990 году был разработан первый код, который мутирует при заражении, а также сохраняет исходный алгоритм на месте. Полиморфный вирус был разработан, чтобы избежать обнаружения. Из-за этого пользователям компьютеров было труднее узнать, что он там есть [20].

Вирус DiskKiller был выпущен журналом PC Today, предназначенным для пользователей компьютеров. Он заразил тысячи компьютеров. Издание журнала предлагало диск подписчикам. Они заявили, что это был несчастный случай, и они не знали, что существует риск [13].

В 1996 году была разработана возможность скрытности. В том же году были выпущены макровирусы. И то, и другое создало больше проблем и потребовало новых разработок антивирусного программного обеспечения. Начиная с первого антивируса, целью было увеличить количество способов защиты от рисков. По мере того, как одна хакерская группа развивалась за другой, компании сталкивались с множеством проблем, связанных с повышением безопасности и минимизацией утечек данных.

На подходе были и другие типы вредоносных программ. Вирус ILOVEYOU и Melissa заразили миллионы компьютеров в 1990-х годах, нацеленных на Microsoft Outlook. Эти вирусы вызывали значительное замедление работы и отказы почтовых систем [13].

В то время многие из циркулирующих вирусов искали финансовую выгоду. Некоторые нацелены на достижение стратегических целей. Тем не менее, было много случаев, когда люди страдали от потери данных, финансовых потерь или других рисков из-за этих вирусов. Основные новостные сообщения подхватили это в быстром темпе. Это приводит к еще большему давлению на создание решений для кибербезопасности. В результате компьютерная безопасность стала большим бизнесом.

В последующие годы были разработаны новые стратегии, помогающие справиться с растущими проблемами. Одним из них был Secure Socket Layer. Он был разработан как способ защиты пользователей Интернета. Secure Socket Layer (SSL) был введен в действие в 1995 году. Он помог защитить такие действия, как онлайн-покупки. Netscape разработал для него протокол. Позже он станет основой для разработки безопасного протокола передачи гипертекста (HTTPS) [20].

Рост Интернета был невероятным в этот период. Компьютеры были практически в каждом доме и офисе. Хотя это помогло потребителям, оно создает больше рисков и возможностей для преступников.

В начале десятилетия появился новый тип заражения, при котором больше не было необходимости загружать файлы. Достаточно было просто зайти на зараженный вирусом сайт. Этот тип скрытого вредоносного ПО был разрушительным. Он также проник в службы обмена мгновенными

сообщениями.

В это же время возникла и первая хакерская группа. В эти группы обычно входят люди с определенными хакерскими навыками. Они могут начать кампанию кибератаки с различными целями. Один из первых стал более узнаваемым, когда взломал Церковь Саентологии. Для этого он распространял атаки типа «отказ в обслуживании» (DDoS-атака). Группа под названием Anonymous продолжает проводить атаки на различные высокопоставленные цели [13].

Взломы кредитных карт также происходили в 2000-х годах. Это связано с утечкой данных, нацеленной на кредитные карты. Группа Альберта Гонсалеса имела особое значение. Этой группе удалось украсть конфиденциальную информацию с 45,7 млн кредитных карт. Они получают доступ через базу данных продавца. Это создало более широкую необходимость сосредоточиться на информационной безопасности в различных секторах, включая розничную торговлю [13].

Атаки на Yahoo также происходили в это время. В 2013 и 2014 годах они стали известны. В одном случае более 3 миллиардов человек с учетной записью Yahoo были взломаны. Для этого хакеры использовали методы целевого фишинга. Это создало возможность неограниченного доступа к бэкдору [21].

Атаки, спонсируемые государством, являются еще одной проблемой. За ними следит Центральное разведывательное управление США (ЦРУ) [21].

Киберугрозы продолжают развиваться, но при этом, также разрабатывались решения. Разработаны новые методы обнаружения. Были созданы новые решения для предотвращения угроз. Это включало использование новых технологий и подходов. Вот некоторые примеры:

- Компьютерная криминалистика
- Многофакторная аутентификация
- Сетевой поведенческий анализ (NBA)
- Защита в режиме реального времени
- Аналитика угроз и обновленная автоматизация
- Песочница
- Резервное копирование и зеркалирование
- Многовекторные атаки
- Социальная инженерия
- Брандмауэры веб-приложений

Угрозы кибератак многочисленны. Они продолжают присутствовать. Фишинг, потеря личных данных в Интернете и атаки программ-вымогателей часто происходят во всем мире. Тем не менее, поиск способа свести к минимуму нарушения безопасности стал более важным, чем когда-либо.

Искусственный интеллект и машинное обучение — это два инструмента, которые могут найти свое применение в кибербезопасности. Усилия по предотвращению атак необходимы сегодня для многих компаний. В результате необходимость делать это более глубоким и эффективным образом зависит от новых технологий. Это лишь некоторые из доступных решений. Возможно,

потребуется разработать много новых решений для автоматизации процесса. Вот почему развитие новых навыков так важно в отрасли. Индустрия кибербезопасности продолжает расти и процветать. Новые технологии помогают минимизировать риски. Опережение угроз имеет решающее значение. Для этого часто требуются высококвалифицированные специалисты в отрасли.

Несмотря на то, что Эстония стала одной из самых развитых стран на постсоветском пространстве в области информационных технологий, 25 апреля текущего сайты Эстонии подверглись кибератаки. К счастью, вредоносные запросы перехватывались до того, как достигнут цели и выведут из строя компьютерные системы.

Сам Департамент государственной инфосистемы Эстонии (RIA) также стал мишенью для кибератаки, однако ее удалось отразить.

Данный кейс показывает, что правительство любой страны может быть атаковано, но степень нанесенного ущерба уже зависит от готовности национальной системы информационной безопасности. В случае Эстонии, все угрозы предотвращены своевременно, без значительного ущерба для общества и государства. Сможет ли Казахстан также справиться с новыми вызовами инновационных достижений покажет время.

1.2 Теоретико-правовые аспекты кибербезопасности

Кибербезопасность выходит за национальные границы во многих отношениях. Техническая инфраструктура интернета носит глобальный характер. Злоумышленники, базирующиеся в одной стране, могут скрыть свою личность, взяв под контроль компьютеры в других странах. Глобальные компании продают программное обеспечение, оборудование и услуги по обеспечению безопасности, которые могут создавать уязвимости или бороться с ними по всему миру. Даже самая кибер-подкованная страна не может полностью защитить себя. Единственным абсолютным решением на сегодня остается тотальный отказ от использования информационными технологиями, отключение от глобального интернета. Данный сценарий практически невозможен в любой развитой стране, учитывая катастрофические последствия для национальной экономики, вооруженных сил и всех других систем, зависящих от передовых информационных технологий.

Международное сотрудничество для повышения кибербезопасности — гораздо более реалистичный и жизнеспособный путь. Обмен информацией является наиболее пропагандируемым видом международного сотрудничества, но очень мало известно о том, какой тип информации о кибербезопасности в настоящее время и кому передается, для каких целей и на каких условиях.

В рамках проекта рассматривается анализ общедоступных межправительственных соглашений по кибербезопасности, какую информацию страны обязались предоставить в рамках этих соглашений, какие существуют пробелы.

Формальные соглашения о совместном использовании киберпространства и меморандумы о взаимопонимании являются важной частью основы для

разработки норм сотрудничества в области киберпространства.

За последние несколько лет на различных международных площадках неоднократно заявлялось, о необходимости обмена информацией, развитии новых подходов к разработке национальных стратегий кибербезопасности, механизмах реагирования. Все это может повысить взаимную кибербезопасность при одновременном снижении рисков недопонимания и конфликтов.

Условно все соглашения делятся по следующим направлениям:

Обучение – Соглашения, предусматривающие обучение персонала, либо взаимное, либо в одном направлении.

Исследования — соглашения, предусматривающие совместную работу по исследованию рисков, угроз, методологий обнаружения вторжений и т. Д

Политика — общие соглашения о сотрудничестве, которые включают обмен информацией о политике кибербезопасности, законах, выявление критически важной инфраструктуры на межправительственном уровне.

Обмен информацией — самый общий из типов соглашений, начиная от политические соглашения к соглашениям между агентствами об обмене широкой или расплывчатой информацией о кибербезопасности.

Военные – соглашения, определяющие сотрудничество между министерствами обороны и/или военными силами.

Кибероперации — соглашения, в которых участвуют страны, работающие вместе над предотвращением нарушений кибербезопасности, созданием киберзащиты, техническое сотрудничество в области защиты, обнаружения и реагирования на инциденты, а также соглашения между CERT.

Киберпреступность — соглашения об обмене информацией, координации защиты и реагирования и/или совместные расследования киберпреступлений.

Передовой опыт — соглашения, предусматривающие обмен передовым опытом в области киберзащиты, уведомлений, реагирования на инциденты, восстановления и т. д

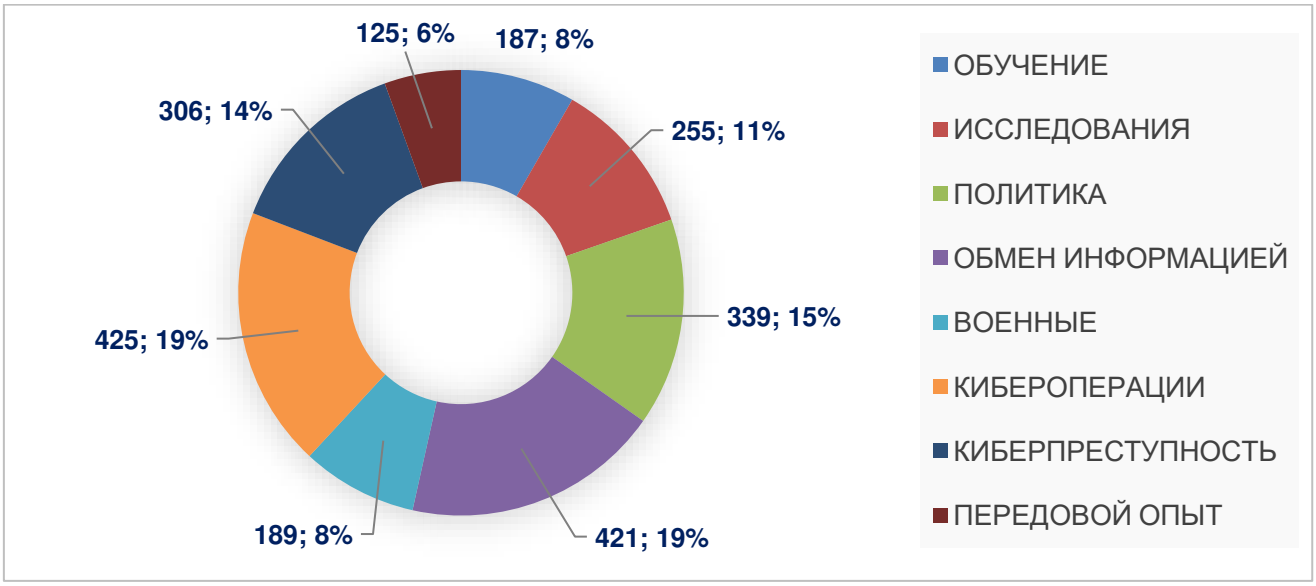

Рисунок 1 – Межправительственные соглашения по направлениям

Примичание – составлено автором на основе данных International Cybersecurity Information Sharing Agreements [23]

Этот обзор соглашений по направлениям (Рисунок 1) показывает, что в настоящее время большая часть обмена киберинформацией (19%) находится на приоритетном уровне, поскольку государства пытаются улучшить свои собственные национальные технические возможности, политику и подходы, перенимая опыт у других стран. Большое количество соглашений о кибероперациях (19%) показывает, что улучшение технических навыков занимает важное место в повестке дня многих государств, и отражает существование множества соглашений в рамках CERT. Большое количество соглашений о киберпреступности (14%) также легко объяснимо, поскольку преступность в киберсфере находится на международной повестке дня с конца 1990-х годов и является ареной, где у большинства государств есть сильные стимулы для сотрудничества [23].

Меньшее количество государств сотрудничает в области военной деятельности (8%) и сетевой защиты, связанной с национальной безопасностью. Это неудивительно, учитывая, что секретность в отношении возможностей национальной безопасности в киберсфере в настоящее время считается первостепенной, особенно в связи с тем, что многие страны стремятся использовать киберинструменты для наступательных военных операций, но это может быть недальновидно. Этот фактор сильно влияет на успех сотрудничества по повышению общего уровня международной кибербезопасности.

Страны по активности международного сотрудничества в области кибербезопасности можно разделить на 3 категории:

Низкий уровень. Группа с самым большим количеством стран (71 государство) [23]. Страны, которые имеют только несколько договоренностей о сотрудничестве, как правило, в качестве членов региональной или субрегиональной договоренности. Казахстан относится к данной категории, учитывая наличие нескольких соглашений в рамках союзов ОДКБ, СНГ, ШОС.

Средний уровень. Страны (40 государств), которые насчитывают до 30 соглашений по кибербезопасности. Эта группа состоит в основном из западных стран, а также из нескольких особо активных членов Ассоциации государств Юго-Восточной Азии, включая Китай (23 соглашения) и Японию (26 соглашений). Члены НАТО и страны-партнеры составляют основную часть этой категории. Одним неожиданным членом является Малайзия (24 соглашения) [23]. Возможно, это связано с его статусом географического кабельного узла для интернет-коммуникаций в регионе. Еще одним сюрпризом является Индия, у которой 29 соглашений, несмотря на ее относительный статус новичка в усилиях по кибербезопасности. Россия находится в нижней части этой группы, имея всего 12 соглашений [23].

Высокий уровень: Категория с наименьшим количеством стран, но количество имеющихся соглашений превышает 30: США (51 соглашение),

Великобритания (42 соглашения), Нидерланды (38 соглашений), Испания (35 соглашений) и Франция (30 соглашений). Правительства этих стран сделали кибербезопасность приоритетным вопросом [23].

Противоборство основных геополитических конкурентов.

Как во многих других вопросах, Россия, Китай и США имеют кардинальные разногласия по вопросам международной кибербезопасности, что создает значительные барьеры для создания глобальной системы сотрудничества в этой сфере.

Напряжение основано не только на опасениях по поводу кибершпионажа с целью получения экономической или политической выгоды и потенциального военного использования киберинструментов во время войны, но и на фундаментальном понимании самой проблемы. В то время как США выступают за свободу слова, глобальный доступ к информации и многосторонний подход к управлению Интернетом, Китай и Россия настаивают на усилении «национального суверенитета» в киберсфере, что означает право на обеспечение контроля над информационным контентом, доступным для их граждан.

Более того защита национальной политической сферы от внешнего вмешательства от подрывной информации. Например, в то время как США и большинство западных стран используют термин «кибербезопасность» для обсуждения защиты сетей и отдельных лиц от кибервторжений, Китай и Россия (и некоторые развивающиеся страны) используют термин «информационная безопасность» для охвата не только защиты данных, но и также защита контента и использование информации, признанной в соответствии с национальным законодательством преступной, что может включать обмен информацией, критикующей политику и действия правительства.

Россия и Китай, в 2011 году под эгидой Шанхайской организации сотрудничества (ШОС) направила в Совет безопасности ООН проект документа «Международный кодекс поведения в области информационной безопасности», в 2015 году вносилась на рассмотрения обновленная версия документа.

Западные страны считают, что нормы в данном документе угрожают правам и свободам граждан в информационном поле, позволяют национальным правительствам контролировать контент.

Предложение Кодекса было отклонено большинством западных государств. Этот идеологический раскол не нов для информационного века, но отражает давнюю напряженность между различными социальными конструкциями в отношении прав и обязанностей граждан по отношению к государству и центральному правительству.

На многостороннем уровне из-за этого фундаментального разрыва Россия и Китай продолжают играть ведущую роль в продвижении концепции государственного контроля в кибер пространстве на различных площадках, в том числе в рамках деятельности ГПЭ Совета безопасности ООН при обсуждении норм поведения по процессам информационной безопасности в рамках Международного союза электросвязи и по вопросу управления Интернетом.

Активность в киберпространстве между крупными мировыми державами

отражает эти различия в идеологии и геополитических целях. Например, западные государства-единомышленники наиболее открыто делятся друг с другом информацией по всем категориям, включая политические соглашения, отстаивающие права человека и свободу информации в киберсфере. Россия, с другой стороны, имеет ограниченный обмен информацией о киберпреступности из-за того, что считает, что разрешение участия внешних государств в расследовании преступного поведения в киберсфере может поставить под угрозу ее национальный суверенитет, детальное распределение межправительственных соглашений США, Китая и России по направлениям изображено на Рисунке -2.

Китай и Россия подписали соглашения, направленные на расширение их возможностей, а также возможностей других государств-единомышленников на уровне центрального правительства блокировать определенную информацию от взглядов широких слоев населения.

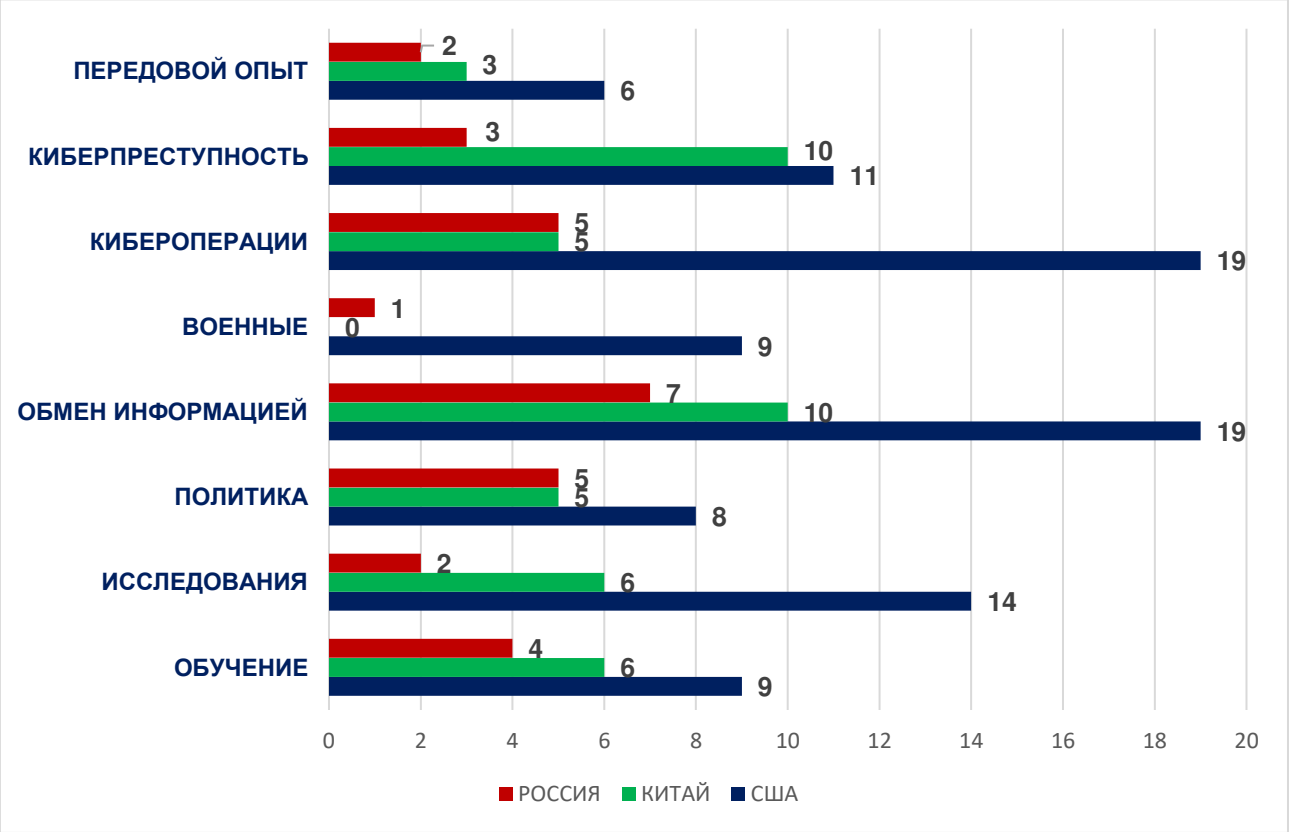

Рисунок 2 – Распределение межправительственных соглашений США, Китая и России

Примечание – составлен автором на основе данных International Cybersecurity Information Sharing Agreements [23]

Как следует из рисунка 2 в Соединенных Штатах на сегодняшний день заключено наибольшее количество соглашений о совместном использовании киберпространства. Обмен информацией, исследования и кибероперации являются категориями с наибольшей активностью, за которыми следует киберпреступность. В военной категории девять соглашений, не считая

Политики киберзащиты НАТО в целом. За последнее десятилетие США были наиболее активны в работе с другими странами, как для достижения соглашений о совместном использовании, так и для наращивания потенциала в киберсфере (включая повышение киберграмотности и использование информационно-коммуникационных технологий) среди союзных и дружественных стран. Официальные лица США говорят, что Агентство национальной безопасности (АНБ) регулярно информирует страны-союзники, когда обнаруживает против них кибероперации. Например, весной 2017 года АНБ связалось с предвыборным штабом Эммануэля Макрона во время президентских выборов во Франции после того, как обнаружило предполагаемое вмешательство России.

США являются ведущим сторонником модели управления Интернетом с участием многих заинтересованных сторон. Страна больше всего инвестировала в интернет-экономику и имеет самую передовую внутреннюю интернет-архитектуру, такого внимания к техническому сотрудничеству, возможно, и следовало ожидать.

В Китае наиболее распространенными являются киберпреступления, передовой опыт и обмен информацией. Китай имеет 15 двусторонних соглашений с 12 странами — включая рамочное соглашение 2015 года с США, четыре из которых с Индонезией и два с Россией. Индонезийские соглашения сосредоточены на борьбе с киберпреступностью и наращивании потенциала. У Китая нет военных соглашений; однако в новостных сообщениях в конце января 2016 года высокопоставленный индонезийский чиновник в области кибербезопасности заявил, что Китай и Индонезия «реализуют» свои соглашения о сотрудничестве в области кибербезопасности, проведя симуляции кибервойны и учения по урегулированию кризисов в рамках ожидаемого Меморандум о взаимопонимании с Администрацией киберпространства Китая [23].

В последнее десятилетие Китай проявляет интерес к заключению соглашений о совместном использовании киберпространства с западными странами. В том числе соглашением с США в сентябре 2015 года, которое включает обязательство воздерживаться от экономического шпионажа, с Великобританией в октябре 2015 г. и с Германией в июне 2016 г.

Китайская интернет-компания Huawei в феврале 2016 г. Подписала свое первое соглашение с западной страной, Испанией. Соглашение с Испанским национальным институтом кибербезопасности (INCIBE) предусматривает обмен информацией о киберзащите и передовом опыте, а также предусматривает обучение испанских технологов. У нее также есть соглашение CERT-to-CERT с Австралией и соглашение с Южной Кореей от 2014 года, которое охватывает совместное реагирование на киберинциденты, такие как DDoS-атаки, и обмен информацией об угрозах [23].

Китай имеет два двусторонних соглашения. Первое с Россией, в рамках соглашения ШОС. Это соглашение направлено на установление государственного контроля в киберсфере, предотвращение «информационных преступлений» и обмен технологиями, направленными на мониторинг контента

и защиту внутренних сетей от информации, считающейся вредоносной. Всеобъемлющее китайско-российское соглашение было подписано в апреле 2015 г.

Второе соглашение, заключено в то же время, между «Лабораторией Касперского» и Zhongguo Wangan, подразделением государственной China Electronics Technology Group Registration (CETC), о сотрудничестве в области программного обеспечения для предотвращения кибератак. Сделка предназначена для помощи Китаю в создании программного обеспечения для защиты от вредоносных программ.

В соответствии со своими опасениями по поводу государственного контроля над контентом и «информационной войны» с 1998 года Китай строит свой так называемый «Великий брандмауэр» для проверки и блокировки входящего интернет-контента. Это включает в себя блокировку доступа к основным веб-сайтам, таким как Google и Facebook, и попытки заменить такие сайты местными вебсайтами (Baidou для Google и Weibo для Facebook), которые тщательно контролируются службами безопасности. Парламент Китая принял новый закон в ноябре 2016 года. Закон направлен на борьбу со взломом китайских правительственных и отраслевых сетей и вызвала протесты со стороны правозащитников и иностранных компаний, работающих в Китае. Наиболее спорные положения закона включают требования к «операторам критической информационной инфраструктуры» хранить личную информацию и бизнес-данные в Китае, оказывать «техническую поддержку» органам безопасности и проходить проверки национальной безопасности для продолжения деятельности [23].

У России самой большой категорией является обмен информацией. Россия имеет двусторонние соглашения только с восемью странами. Только одно российское соглашение попадает непосредственно в категорию военных, двустороннее соглашение с Ираном, которое включает обмен разведывательной информацией, взаимодействие против угроз и совместную оборонную деятельность.10 Интересно, что у России есть два отдельных соглашения с Японией, датированные 2013 и 2014 годами, которые подпадают под категории «Обучение» и «Обмен информацией».

Россия очень мало взаимодействует в категории киберпреступлений, которая в целом является одной из крупнейших категорий. Таких соглашений у Москвы всего три: с Индией, Ираном и ШОС. Это отражает враждебное отношение России к разрешению другим странам помогать в отслеживании базирующихся в России киберпреступников. В связи с чем, Интерпол и нормы Будапештской конвенции 2001 г. (первый договор о киберпреступности, разработанный Советом Европы) в случае трансграничных преступлений бессильны, из-за опасений относительно национального суверенитета. Совместные усилия России и США, вылившиеся в пакет соглашений в 2013 году, были приостановлены после украинского кризиса. Однако представители России и США встретились в апреле 2016 г. в Женеве, чтобы попытаться оживить сотрудничество [23].

Для определения состояния дел в области кибербезопасности применяется Глобальный индекс кибербезопасности (далее - ГИК), который разработан МСЭ. Под состоянием дел в области кибербезопасности понимается описание возможностей страны, организации или компании для обеспечения кибербезопасности. ГИК является инструментом наращивания потенциала, который оценивает приверженность стран делу обеспечения кибербезопасности, определяет их состояние дел в области кибербезопасности и аспекты, требующие улучшения. Состояние дел стран в области кибербезопасности может оцениваться на основе пяти принципов, определенных в Программе МСЭ [24]. В частности, страны получают баллы ГИК в зависимости от уровня их приверженности этим пяти принципам. Эти оценки относят страны в группы:

- начинающие. Страны, которые делают первые шаги, демонстрирующие их приверженность этим принципам;
- развивающиеся. Страны, которые привержены этим принципам;
- ведущие. Страны, принявшие высокие обязательства в отношении этих принципов.

Вместе с тем, существует альтернативная оценка состояния дел стран в сфере кибербезопасности (Cybersecurity Capacity Maturity Model) (далее - CMM), разработанная Глобальным центром создания потенциала в области кибербезопасности (GCSCC) при Оксфордском университете.

Оценка определяется путем изучения усилий стран в таких областях, как «нормативное регулирование и стратегия в области кибербезопасности», «киберкультура и общество», «образование, обучение и навыки в области кибербезопасности», «нормативно-правовая база», а также «стандарты, организации и технологии». Эта оценка позволяет странам получить информацию об уровне зрелости их потенциала:

1. Начальный уровень: когда кибербезопасность отсутствует или только начинает развиваться;
2. Формирующийся уровень: когда существует некоторая кибербезопасность;
3. Установленный уровень: когда кибербезопасность существует, но уделяется минимальное внимание вопросу выделения ресурсов);
4. Стратегический уровень: когда осознанный и взвешенный выбор в отношении кибербезопасности;
5. Динамичный уровень: когда меры обеспечения кибербезопасности адаптируются к изменениям условий и потребностей [25].

Модель CMM использовалась для оценки во всем мире по отдельности или в рамках регионального исследования (Global Cyber Security Capacity Centre, 2018). В дополнение к модели CMM, Глобальный центр создания потенциала в области кибербезопасности разработал портал Cybersecurity Capacity Portal, который содержит материалы по созданию потенциала в области кибербезопасности, информацию о передовой практике и облегчает обмен информацией, чтобы помочь странам улучшить состояние дел в области кибербезопасности.

В ноябре 2001 года Советом Европы принята Конвенция о киберпреступлениях [26]. На сегодняшний день это соглашение включает наибольшее количество стран, которые придерживаются принятых в данном документе норм. Россия и Китая не являются участниками этого соглашения.

Будапештская конвенция регламентирует процессы международного характера, касающиеся преступлений совершенных в киберпространстве. К таким преступлениям относятся нарушения авторских прав, мошенничество с применением информационно-коммуникационных технологий, детская порнография и тд. Казахстан не является участником данной конвенции.

1.3 Современные угрозы кибербезопасности

Что такое киберугроза? Для эксперта по кибербезопасности определение киберугрозы, данное в Оксфордском словаре, немного не соответствует действительности: «Возможность злонамеренной попытки повредить или нарушить работу компьютерной сети или системы». Это определение будет неполным без включения попытки повредить или украсть данные и нарушить цифровые операции.

Киберугрозы становятся все более изощренными и интенсивными на фоне растущего уровня удаленной работы, миграции в облако и продвинутых киберпреступников. На сегодняшний сохраняются 5 наиболее распространенных кибератак.

- Социальное инженерия
- Программы-вымогатели
- ДДоС атаки
- Дополнительное программное обеспечение
- Облако вычисления уязвимости

Киберугрозы охватили весь 2021 год, и они не собираются прекращаться.

Пандемия COVID-19 стала серьезной проблемой для служб безопасности. Удаленная работа расширила поверхность атаки, заставив службы безопасности защищать гораздо большую территорию, чем раньше. Во время пандемии киберугрозы и утечки данных стали более изощренными и объемными, при этом количество утечек увеличилось на 273% в первом квартале по сравнению с 2019 годом [27].

При выявлении киберугрозы важно знать противника и понимать связанные с ним тактики, техники и процедуры (TTP). TTP субъектов угроз постоянно развиваются, чтобы избежать обнаружения, но источники киберугроз остаются прежними. Всегда есть человеческий фактор; тот, кто попадется на хитрый трюк. Но что еще более важно, всегда есть мотив. Это реальный источник киберугрозы. Понимание TTP злоумышленника определяет мотив киберугрозы и меры необходимые для предотвращения вероятных следующих шагов.

Наиболее распространенные источники киберугроз

- Преступные группы
- Хакеры

- Вредоносный Инсайдеры
- Корпоративный Шпионы
- Государтсва
- Террористы
- Хактивисты

Современные субъекты угроз, такие как организованные киберпреступники, национальные государства и корпоративные шпионы, представляют наибольшую угрозу информационной безопасности для предприятий сегодня. Многие организации изо всех сил пытаются обнаружить эти угрозы из-за их скрытого характера, сложности ресурсов и отсутствия глубокого понимания поведения злоумышленников. Для предприятий эти более изощренные, организованные и настойчивые субъекты угроз видны только по цифровым следам, которые они оставляют после себя. По этим причинам предприятиям необходима широкая видимость за пределами их сетевых границ передовых угроз, конкретно нацеленных на их организации и инфраструктуру.

Атака SolarWinds, обнародованная в декабре 2020 года, стала огромным тревожным звонком для уровня изощренности, используемой хакерскими коллективами. По данным Wall Street Journal:

«Атака сочетала в себе необычайно скрытную коммерческую хитрость с использованием киберинструментов, никогда ранее не применявшихся в предыдущей атаке, со стратегией, которая сосредоточилась на слабом звене в цепочке поставок программного обеспечения, на которое полагаются все американские предприятия и государственные учреждения — подход, который эксперты по безопасности уже давно используют . опасаются, но тот, который никогда не применялся против целей США таким согласованным образом».

Обнаружение угроз может быть затруднено, поскольку киберпреступники используют все более совершенные TTP при эксплуатации жертв. Эти новые меры вынудили организации модернизировать аналитические и операционные инструменты, навыки и процессы безопасности, чтобы оставаться впереди. Многие группы операций по обеспечению безопасности сталкиваются с серьезными проблемами. Они часто работают с разрозненными точечными инструментами и ручными процессами, но им не хватает опыта, ресурсов и навыков, чтобы идти в ногу с меняющимся ландшафтом угроз.

2 О ДЕЙСТВУЮЩЕЙ СИСТЕМЕ КИБЕРБЕЗОПАСНОСТИ И ПОТЕНЦИАЛЬНЫХ УГРОЗАХ В РЕСПУБЛИКЕ КАЗАХСТАН

2.1 Система кибербезопасности в Казахстане

Казахстан активными темпами осваивает цифровое пространство. В 2017 году утверждена государственная программа «Цифровой Казахстан» (далее - программа).

Программа разработана с целью повышения качества жизни каждого казахстанца, путем совершенствования процессов жизнедеятельности через внедрение передовых информационных технологий. Более подробно система кибербезопасности в Казахстане изображена на рисунке – 3.

Рисунок - 3 – Система кибербезопасности в Казахстане

Примечание – составлено автором

Реализация задач поставленных в Программе способствовала не только диджитализации большого количества сфер жизнедеятельности казахстанцев, но и созданию дополнительных рисков связанных с информационными технологиями.

Осознавая риски национальной безопасности, вытекающие из повсеместной цифровизации государственного и частного сектора правительством Казахстана принята Концепция кибербезопасности "Киберщит Казахстана" (далее – Концепция).

В рамках Концепции поставлены 6 конкретных и измеримых задачи, которые должны быть достигнуты в текущем году [28]:

1) глобальный индекс кибербезопасности. Казахстан должен войти в 2022

году в ТОП 30 стран по уровню кибербезопасности;

2) В 2022 году 20% населения должно быть осведомлено о возможных рисках, связанных с угрозами в киберпространстве;

3) В 2022 году 800 человек должны пройти переподготовку в области информационных технологий по вопросам кибербезопасности;

4) расширение присутствия национальных производителей по обеспечению программного оборудования и систем в государственных и квазигосударственных организациях до 50%;

5) абсолютное применение сертификатов безопасности, которые были разработаны в Республики Казахстан для информационных ресурсов использующие домены «KZ» и «ҚАЗ»;

6) подключить все информационные системы к центрам по мониторингу информационной безопасности [28].

Обе программы в текущем году заканчиваются и уполномоченным органам предстоит достигнуты ли поставленные цели.

В рамках исследования проведен SWOT – анализ реализации программы (Рисунок 4).

Рисунок 3 – SWOT – анализ реализации Концепции «Киберщит»

Примечание – составлено автором

К примеру, индикатор «Глобальный индекс кибербезопасности» является универсальным для обоих программ. На сколько данный показатель отражает реальную ситуацию готовности страны к киберугрозам. Мнения экспертного сообщества по этому вопросу отличаются.

«Почему он важен? Потому что за счет такой небольшой строчки как индекс киберготовности, можно сказать, подтягивается вся сфера», — пытается

объяснить логику присутствия индекса в госпрограммах Олжас Сатиев, президент ОЮЛ «Центр анализа и расследования кибератак» (ЦАРКА) [29].

В 2015 году изучение вторичных данных позволило исследователям поместить Казахстан на 23-е место из 29. На той же позиции оказались, к слову, еще 14 стран, среди которых была, например, Сирия, уже четвертый год находившаяся в состоянии гражданской войны. В 2017 году авторы индекса отказались от идеи группировать страны со схожими показателями, и Казахстан занял 82-е место из 164. В 2019 году республика расположилась уже на 40-м месте из 175. В отчете за прошлый год Казахстан поднялся до 31-й строчки в рейтинге из 193 стран [29].

Сабина Садиева, заместитель директора Казахстанского института стратегических исследований при президенте, убеждена, что глобальные индексы не подходят для национальных систем управления. По её мнению, они играют «этакую роль заменителя», когда на уровне политического руководства отсутствует оценка эффекта мер госрегулирования на общество и экономику [29].

«В этом плане международные рейтинги — это удобный инструмент. Проблема в том, что инструмент подменяет собой сам результат», — пишет она.

Анна Гусарова, директор Центральноазиатского института стратегических исследований, член Экспертной группы по цифровым правам, тоже считает, что «индекс кибербезопасности не показывает, насколько эффективно были реализованы госпрограммы». Она подчеркивает, что он не отражает глубину проблем, которые в этой сфере есть в самых отдаленных уголках республики. Кроме этого, ориентация на индекс лишь подстегивает убыстряющийся темп цифровизации страны [30].

Преобладающая роль государства, чрезмерный акцент на технологические аспекты и необходимость получения быстрых количественных результатов — в этом заключается специфика цифровизации в Казахстане. Такой нестратегический подход чреват неприятностями, пишут Гусарова и Серик Джаксылыков в своем исследовании, посвященном защите персональных данных [30].

«С одной стороны, речь идет об уязвимостях, исходящих от государственных и негосударственных игроков», — утверждают исследователи.

Уязвимость — это недостаток в компьютерной системе, использование которого приводит к нарушению целостности системы и некорректной работе. В том, что таких недостатков в отечественных системах достаточно, казахстанцы убеждаются все последние годы.

В 2019 году персональные данные 11 млн казахстанцев утекли с серверов Центральной избирательной комиссии. В 2020 году специалисты ЦАРКА обнаружили утечки данных из Генеральной прокуратуры и Системы контроля качества в сфере здравоохранения. В том же году команда «белых» хакеров проверила на наличие уязвимостей 91 государственный веб-ресурс [29] (результаты на Рисунке - 4).

Рисунок 4 – Результаты мониторинга уязвимостей 91 государственных ресурсов, по данным ЦАРКА

Примечание – Источник: результаты исследования по уязвимостям государственных ресурсов проведенное ЦАРКА [29]

В 2021 году независимые исследователи во время поиска уязвимостей обнаружили доступ к системе управления жизнеобеспечением столицы, а также выяснили, что при получении результатов ПЦР-тестирования можно получить медицинские данные порядка 7 млн граждан, обратившихся в одну из лабораторий страны [30].

«С другой стороны, отсутствует видение по формированию культуры цифровизации, продвижению кибергигиены и цифровой грамотности среди граждан», — исследователи называют еще один недостаток выбранной Казахстаном модели цифровизации.

В 2017 году правительство представило программу «Цифровой Казахстан». В ней пять направлений диджитализации и ни в одном из них не говорится о необходимости защиты персональных данных и продвижении цифровой культуры [31].

В 2021 году исследовательница Алия Тлегенова решила выяснить отношение гражданского общества к официальным мерам по защите персональных данных и получила вполне закономерные результаты. Она отправила форму с опросом в 160 отечественных НПО. Ответ пришел лишь от 24 организаций, и только в трети сотрудники проходили тренинги по информационной безопасности и кибергигиене [29].

«Человеческий фактор все еще остается самым слабым звеном в цепочке цифровой безопасности. По разным данным, 95% всех киберинцидентов происходит именно из-за беспечности человека», — Валерий Зубанов, коммерческий директор «Лаборатории Касперского» в Центральной Азии [32].

Между тем, среди целевых индикаторов программы «Цифровой

Казахстан» можно обнаружить рост производительности труда и созданных рабочих мест, долю электронных госуслуг и интернет-пользователей, объем инвестиций в стартапы и улучшение в индексе глобальной конкурентоспособности. «Киберщит Казахстана», помимо прочего, нацелен на увеличение количества переподготовленных IT-специалистов и доли отечественных программных продуктов, используемых в госсекторе.

Анна Гусарова пока затрудняется прогнозировать, к чему приведет выбранная Казахстаном траектория цифровизации, однако уверена – пандемия COVID-19 убедительно продемонстрировала весь масштаб имеющихся в отрасли проблем. При этом эксперт не склонна возлагать всю ответственность на государство — патернализм казахстанцев тоже ощутимо тормозит процесс развития кибербезопасности.

«На данном этапе я не вижу совместного желания со стороны государства, бизнеса и гражданского общества работать в этой сфере», — говорит исследовательница [30].

В части кибербезопасности можно создать «хороший прецедент», объединив усилия и экспертизу всех стейкхолдеров. Первопроходцами в этом, вероятно, можно считать Экспертную группу по цифровым правам и инициативу BugBounty.kz. Первая в Казахстане продвигает повестку соблюдения прав человека в цифровой среде, а вторая – налаживает связь между IT-сообществом, государством и крупным бизнесом.

При этом истинной целью этого диалога должен стать поиск пресловутого баланса между уважением свобод граждан и обеспечением национальной безопасности в виртуальном пространстве. Ни у одной страны мира пока нет универсальной формулы — идеального соотношения прав и ограничений в киберсреде. Поэтому ценность постоянного обмена мнениями в этом контексте не теряет своей актуальности и спустя полвека после появления интернета.

Деятельность государственных органов и активность частного сектора способствовала росту цифровизации большого количества процессов в обществе, а также повышению эффективности мероприятий, направленных на обеспечение защищенности информации в киберпространстве.

Вместе с тем, остается открытым вопрос ответственности за неправомерные действия в сети интернет. Более того, такая проблема остается актуальной во всем мире. Как известно, безответственность порождает безнаказанность, а безнаказанность порождает вседозволенность.

Нормы законодательства Республики Казахстан предусматривают несколько видов юридической ответственности. Среди них традиционно выделяют уголовную, административную, дисциплинарную, гражданско-правовую и материальную ответственности.

В рамках проекта рассматривается форма уголовной ответственности за нарушения норм поведения в киберпространстве. В национальном уголовном ном законодательстве имеются следующие нормы, регламентирующие правонарушения в киберпространстве.

Глава 7. Уголовные правонарушения в сфере информатизации и связи

Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций.

Статья 206. Неправомерные уничтожение или модификация информации.

Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций.

Статья 208. Неправомерное завладение информацией.

Статья 209. Принуждение к передаче информации.

Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов.

Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа.

Статья 212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели.

Статья 213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства.

Часть 3 статья 147 УК РК. Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите. Часть 3. Деяния, предусмотренные частью второй настоящей статьи, совершенные лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сети телекоммуникаций, либо в целях извлечения выгод и преимуществ для себя или для других лиц, или организаций.

Часть 2 статьи 148 УК РК. Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сетям телекоммуникаций.

Пункт 4 часть 2 ст. 188 УК РК. Кража, совершенная путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.

Пункт 4 часть 2 статья 190 УК РК. Мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы.

Пункт 3 часть 3 статья 195 УК РК. Причинение имущественного ущерба путем обмана или злоупотребления доверием путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.

П. 5 ч. 3 ст. 297 УК РК. Незаконные изготовление, переработка, приобретение, хранение, перевозка в целях сбыта, пересылка либо сбыт

наркотических средств, психотропных веществ, их аналогов посредством использования электронных информационных ресурсов.

Пункт 3 часть 2 статья 299 УК РК. Склонение к потреблению наркотических средств, психотропных веществ, их аналогов посредством использования электронных информационных ресурсов.

Пункт 4 часть 3 статья 301 УК РК. Незаконный оборот ядовитых веществ, а также веществ, инструментов или оборудования, используемых для изготовления или переработки наркотических средств, психотропных веществ, их аналогов или ядовитых веществ посредством электронных информационных ресурсов.

По данным отчета Комитета правовой статистики и специальным учетам Генеральной прокуратуры за 2021 год за правонарушения в сфере информатизации и связи зарегистрировано всего 74 уголовных дела, из них в суд направлено 3 [33]. По данным KZ-CERT за аналогичный период совершенно 23773 кибератаки.

2.2 Новые вызовы для безопасности Республики Казахстан в киберпространстве

В рамках исследования проведен PEST-анализ рисков от кибернетических атак для Республики Казахстан.

Таблица 1 – PEST-анализ рисков от кибернетических атак для Республики Казахстан

ПОЛИТИКА	**ЭКОНОМИКА**
Подрыв суверенитета страны	Увеличение расходов на развитие системы кибербезопасности
Вмешательство в выборы Президента в 2024	Угроза национальной банковской системе и всей экономике страны
Политический шпионаж	Вывод капитала за рубеж, путем хищения средств с счетов физических и юридических лиц
Влияние не политических деятелей путем шантажа, либо угрозой смерти	Коммерческий шпионаж
Репутационные риски, связанные с критикой западных партнеров из-за применяемых методов противодействия киберугрозам путем отключения страны от интернета, которые связывают с ограничением гражданских свободы и независимости прессы	Значительный расходы на предотвращение кибератак путем отключения страны от интернета
ОБЩЕСТВО	**ТЕХНОЛОГИИ**
Сбой в работе критически-важных	Сбой в работе национальной

инфраструктурных объектов	информационно-коммуникационной инфраструктуры
Продолжение Таблицы 1	
Деструктивное влияние в социальных сетях	Вынужденное обновление технологической инфраструктуры системы безопасности
Рост недоверия к власти, вызванный неспособностью противостоять хищениям денежных средств с личных банковских счетов	Дестабилизация работы наиболее популярных мобильных приложений (kaspi, egov mobileи тд)
Рост недовольства среди населения в связи с чрезвычайными методами борьбы с кибератаками, путем полного отключения интернета	
Кибербуллинг	
Примечание – подготовлено автором	

В зависимости от целей совершения кибер атаки бывают нескольких видов. Условно, мотивы можно разделить на 2 вида (политические и экономические):

1) Политические. Самая опасная из угроз это потеря государственного суверенитета. К примеру, события 2010-2011 годов, которые произошли в арабских странах в 2010 – 2011 годах. Безусловно, в этих странах были проблемы. В том числе, идеологического, политического и социального характера. Но ключевую роль в событиях сыграли информационные технологии, как инструмент планомерной и структурированной организации оппозиции.

Создается вымышленный персонаж, которого на самом деле нет. Далее идет массированный взброс информации о якобы неправомерных действиях в отношении этого человека со стороны действующего режима.

Например, сирийская блогерша Амина Арраф, которую якобы «похитил сирийский режим в Дамаске». Как стало позже известно, Амина Абдалла Арраф аль-Омари — псевдоним, под которым вёл блог американец, активист движения за мир по имени Том Макмастер. Блог «Лесбиянка из Дамаска» якобы был создан в поддержку гражданских и политических свобод сирийцев. При этом, оказав значительное деструктивное влияние на арабское общество [34].

Другой пример, приход к власти Николы Пашиняна в Армении стал возможным во многом благодаря социальным сетям.

В данном вопросе самое важное, что киберугрозы в этих странах возникли за долго до самих событий. Шпионская деятельность велась без лишнего шума в сети. Собирались персональные данные граждан, у кого какие проблемы, интересы, потребности. Анализировалась работа информационных ресурсов государственных органов и теле-радио вещательных компаний.

В социальных сетях формировались группы по разным интересам:

рыбалка, знакомства, творчество и т.д. Граждане сами того не понимая, становились участниками будущих революционных событий.

В решающий момент формируется антиправительственный информационный фон, при этом сайты госорганов и правительственных СМИ блокируются благодаря ddos, dos – кибератакам. Правительство бессильно, а хаотичное общество превращается в организованную оппозицию.

Такая деятельность сейчас не редкость. К примеру, в июле 2021 года стало известно, хакеры загрузили на сайт электронного правительства Казахстана вирусную программу, которую скачивают пользователи.

Одной из причин уязвимости страны перед киберпреступностью является стремительное развитие информационных технологий.

В настоящее время наблюдается большая эпидемия атак на веб-сайты, и ежедневно по всему миру взламывается более 30 000 веб-сайтов. Когда злоумышленники находят даже малейшую уязвимость в одном из его модулей, он открывает им доступ к более чем 1000 веб-ресурсам. Хакеры используют эти сайты для заражения конечных пользователей, кражи их конфиденциальных личных данных, публикации испорченных веб-сайтов с экстремистскими или террористическими лозунгами или просто используют их как часть своего ботнета для рассылки спама или вирусов. Несмотря на меняющийся ландшафт угроз, только 3% владельцев веб-ресурсов в мире используют функции безопасности [35].

Нашим большим заблуждением является то, что все это происходит где-то далеко за рубежом. Учитывая предстоящие выборы в Казахстане в 2024 году, не нужно быть большим экспертом, чтобы понимать, что подготовительные работы к цифровой войне уже ведутся полным ходом. А Казахстан станет полигоном для испытаний новых цифровых инструментов.

Безусловно, Казахстаном ведется работа по обеспечению кибербезопасности. В 2017 году принята соответствующая концепция «Киберщит», то есть 5 лет назад. Учитывая последствия пандемии, стремительный скачок в мире цифровых технологий, появление новых игроков (zoom, ms teams и др.) остается только догадываться на сколько эта концепция актуальна.

Почти каждый казахстанец ежедневно использует продукты цифровых технологий, владельцами которых являются иностранцы (Yandex, 2Gis, whatsapp, facebook, youtube, Instagram и т.д.). Количество пользователей же растет с каждым днем. На начало 2020 года более 4,5 миллиарда людей пользуются интернетом, а аудитория социальных сетей перевалила за отметку в 3,8 миллиарда [36]. В Казахстане покрытие мобильного интернета составляет уже 99%. А это более чем достаточная аудитория для продвижения собственных интересов [37].

2) Экономические. Другими словами, незаконное обогащение, используя информационные технологии. В данном направлении возможностей очень много. Начиная от элементарной кражи средств с банковской карты и заканчивая блокировкой деятельности бизнес-гигантов, с последующим шантажом.

Приведу примеры: хакеры получили 15 ТБ данных от 8000 организаций, работающих с израильской компанией Voicenter, и предложили данные онлайн за 1,5 миллиона долларов; в ходе одного из крупнейших ограблений криптовалюты хакер украл около 600 миллионов долларов с блокчейн-сайта Poly Network. Затем хакер вернул напрямую 340 миллионов долларов и перевел 268 миллионов долларов в цифровой кошелек, который совместно контролируется им и Poly Network. Однако средства в кошельке остаются недоступными, пока хакер не предоставит цифровой ключ; крупнейшая в мире мясоперерабатывающая компания JBS, базирующаяся в Бразилии, стала жертвой атаки программы-вымогателя. В результате атаки были остановлены предприятия в США, Канаде и Австралии. Атака была приписана русскоязычной киберпреступной группе REvil и тд [38].

В Казахстане, невозможно оценить текущую ситуацию в этой проблеме, так как ее никто не отслеживает должным образом. Вся кибербезопасность сводится к защите государственных информационных ресурсов.

При этом, частные лица и бизнес остаются не защищенные. Для злоумышленников не существует государственных границ и законов. Находясь на другом материке земного шара, они крадут деньги наших налогоплательщиков. Получается, существует стабильный канал вывода капитала из страны, масштабы которого установить невозможно.

Подытоживая вышеописанное, необходимо отметить, что угроза кибербезопасности это неизбежная реальность, которая уже здесь и сейчас. Какими будут последствия зависит, от нас самих, от тех решений, которые мы примим.

ЗАКЛЮЧЕНИЕ

Несмотря на процесс резкой антиглобализации, связанной с пандемией коронавируса, а также с эскалацией международных отношений из-за конфликта на Украине, все понимают необходимость межгосударственного сотрудничества в вопросах кибербезопасности.

В этой связи, в силу стремительно меняющегося мира, роста напряженности между государствами и неизбежного технологический прогресса, в целях недопущения глобального кибертерроризма и демонизации технологического прогресса предлагается рассмотреть следующие меры международного и национального характера.

1. Определить и ратифицировать общие правила игры для всех государств. Наиболее подходящей площадкой для разработки и принятия таких правил является Организация Объединенных наций (ООН). Более того, Советом безопасности ООН такая работа уже ведется не один года, но к консенсусу страны прийти не могут. В настоящее время на рассмотрении находится проект конвенции, подготовленный Российской Федерацией, по некоторым положениям проекта у стран-участниц имеются разногласия.

Для Казахстана развитие двухсторонних межправительственных соглашений видится наиболее эффективным решением в данном контексте.

2. Определить политику реестра IT-специалистов начиная с обучения в учебных заведениях. IT-специалисты должны обучаться и совершенствовать свои навыки во благо людей. Любые другие действия должны быть под международными контролем и жестоко пресекаться. Международный реестр должен хранить информацию об IT специалистах, их квалификации и области специализации, текущее место занятости. Во-первых, это дисциплинирует самих специалистов, во-вторых, облегчит работу правоохранительных органов по выявлению и привлечению к ответственности киберпреступников.

3. Создать систему беспрепятственного обмена опытом и технологиями между всеми участниками интернет пространства, не только правительствами, но и частным сектором. Так как, технологии использованные при атаки на частный сектор сегодня, могут быть использованы против правительства уже завтра.

4. Привлечь IT гигантов (Google, Youtube, Facebook и тд.) к крупномасштабной борьбе с киберпреступностью. Зачастую крупные социальные сети используются для обучения хакерству и обмена отрицательным опытом. Такие вещи должны пресекаться. К примеру, на Youtube можно легко найти курс о том, как взломать аккаунт в социальных сетях. Если бы Google на запрос «Как взломать сайт университета» выдавал бы страницу с предупреждением об уголовной ответственности за киберпреступления, многих инцидентов можно было бы избежать.

5. Казахстану необходимо принимать новую стратегию кибербезопасности. Концепция «Киберщит» очевидно устарела. Стратегия должна охватывать следующие направления:

5.1 Повышение качества человеческого капитала. Открытие новых форм и учебных заведений для подготовки IT специалистов, со стажировкой за рубежом. Для закрепления их на родине, создание комфортных условия для проживания, включая достойную оплату труда, льготные ипотечные займы и другие инструменты нематериальной мотивации;

5.2 Развитие сотрудничества государственного и частного секторов по опыту США. Отечественные структуру ответственные за политику безопасности в стране без преувеличения закрыты. В США частный сектор привлекается для обучения государственного сектора, а также для тестирования государственных информационных систем. Взаимное сотрудничество повышает защиту и предупреждает негативные последствия. Частный сектор более гибок и имеет больше возможностей для всестороннего развития;

5.3 Обязательная интеграция казахстанского IT-сообщества в международные институты по информационной безопасности. Государство со своей стороны, с учетом национальных интересов, обеспечивает присоединение Казахстана к международным межправительственным инициативам по вопросам информационной безопасности (соглашения, конвенции, договора и тд.). Также государство, в рамках своих возможностей и полномочий, оказывает содействие частным организациям и лицам, для интеграции в мировое IT-сообщество;

5.4 Обеспечение национальной правовой базы для создания полноценной системы защиты информационных ресурсов государственного и частного секторов, а также физических лиц. Необходимо пересмотреть положения уголовного и уголовно-процессуального законодательства, с учетом международной практики, для создания эффективной системы привлечения к ответственности злоумышленников как внутри страны, так и за рубежом. Для этого, необходимо развивать инструменты взаимного сотрудничества с другими государствами опираясь на международные конвенции и соглашения;

5.6 Реструктуризация системы защиты от киберугроз. На сегодня за обеспечение информационной безопасности в стране отвечают три государственных органа. Государственная техническая служба при Комитете национальной безопасности (ГТС). Министерство цифрового развития, инноваций и аэрокосмического развития (МЦРиАП), под защитой которого находятся персональные данные граждан РК. Министерство внутренних дел РК (МВД), занимается привлечением к уголовной ответственности за преступления в сфере информационной безопасности. Кроме того, при Министерстве иностранных дел (МИД) функционирует управление международной безопасности. Учитывая, что киберпреступления не имеют государственных границ и могут наносить ущерб нашему государству и гражданам извне, предлагается консолидировать правоохранительный блок МВД и международное сотрудничество МИД в одну структуру. МВД не имеет достаточных возможностей для полноценного уголовного преследования за рубежом, МИД не имеет достаточно полномочий и опыта в расследовании кибер преступлений. Предлагаемую структуру, возможно, создать при Генеральной

прокуратуре РК, так как этот орган имеет больше полномочий, чем МВД, и более достаточный опыт, чем МИД;

5.7 Представление национальных интересов при ООН. В настоящий момент в организации ведется активная работа по правовому регулированию интернет пространства, в котором принимаются участие страны Европы, США, Россия. Более того, на рассмотрение находится проект Конвенции. К сожалению, Казахстан не в доставочной степени представлен в рабочих органах при ООН по обсуждению информационной безопасности. В этой связи, предлагается назначить постоянного представителя при ООН для участия в вышеуказанных рабочих органах.

Описанные мероприятия являются базовыми для создания национальной стратегии информационной безопасности Казахстана. Учитывая, грядущие выборы в Казахстане, нестабильную геополитическую ситуацию, участившиеся применение информационных технологий в политике необходимо принимать срочные меры.

Кибер угрозы — это неизбежная реальность, которая уже здесь и сейчас. Какими будут последствия зависит, от нас самих, от тех решений, которые будут приняты.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Выступление Президента Казахстана К-К. Токаева на заседании Совета Шанхайской организации сотрудничества, 14 июня 2019 года // Официальный сайт Президента Республики Казахстан www.akorda.kz – URL: https://www.akorda.kz/ru/speeches/external_political_affairs/ext_speeches_and_addresses/vystuplenie-prezidenta-respubliki-kazahstan-kasym-zhomarta-tokaeva-na-zasedanii-soveta-glav-gosudarstv-chlenov-shos-v-rasshirennom-formate. Дата обращения 15.12.2021 г.

2 Информационный ресурс позволяющий осуществлять мониторинг киберугроз в режиме реального времени по всему миру // www.threatmap.checkpoint.com – URL:https://threatmap.checkpoint.com/. Дата обращения 12.05.2022 г.

3 «Информационная безопасность: Учебное пособие». Авторы: Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им.Н.И. Лобачевского, 2017. – 9 с.

4 «Glossary of Key Information Security Terms», Richard Kissel, editor, National Institute of Standards and Technology, U.S. Department of Commerce, Computer Security Division, Information Technology Laboratory, Gaithersburg, May 2013. – p.94.

5 «Кибербезопасность и информационная безопасность: сходства и отличия», авторы: Козлова Н.Ш., Довгаль В.А., ежеквартальный рецензируемый, реферируемый научный журнал «Вестник АГУ», Вып. 3 (286) 2021. – стр.91.

6 «What is cybersecurity?», by Sharon Shea, Executive Editor, Alexander S. Gillis, Technical Writer and Editor, Casey Clark, Technology company «TechTarget» // Official website www.techtarget.com – URL: https://www.techtarget.com/searchsecurity/definition/cybersecurity. Дата обращения 24.04.2022 г.

7 Закон Республики Казахстан «О национальной безопасности Республики Казахстан» № 527-IV от 06.01.2012 года (с изменениями и дополнениями по состоянию на 27.12.2021 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет» – URL: https://adilet.zan.kz/rus/docs/Z1200000527. Дата обращение: 09.05.2022 г.

8 «Книга шифров. Тайная история шифров и их расшифровки», автор Саймон Сингх; перевод с англ. А.Галыгина. – М, АСТ:Астель, 2009 г. – стр.17-20.

9 «Atanasoff-Berry Computer», Paul A. Freiberger, Michael R. Swaine., The Encyclopædia Britannica // Official Website www.britannica.com – URL: https://www.britannica.com/technology/Analytical-Engine. Дата обращения 07.05.2022 г.

10 «John von Neumann. Collected works. Volume V. Design of computers, theory of automata and numerical analysis», author J-V. Neumann, general editor A.H. TAUB, Oxford: Pergamon press, 1961 – p.302.

11 «Что такое телефонный фрик?», цифровая энциклопедия Netinbag // Официальный веб-сайт www.netinbag.com – URL: https://www.netinbag.com/ru/technology/what-is-a-phone-phreak.html. Дата обращения 07.09.2022 г.

12 «The Tech Model Railroad Club. Here's where our computer culture was born», author Steven Levy, Back Channelnov, Information portal «Weird», 2014 // official website www.weird.com – URL: https://www.wired.com/2014/11/the-tech-model-railroad-club/. Дата обращения 24.02.2022 г.

13 «History of Cyber Security», Educational web-portal «Cyber-security.degree» // Official website www.cyber-security.degree.com – URL: https://cyber-security.degree/resources/history-of-cyber-security/. Дата обращения: 14.03.2021 г.

14 «Vassar's First Computer», author Grace Murry Hopper, The Vassar Encyclopedia project // Official website www.vassar.edu – URL: https://www.vassar.edu/vcencyclopedia/curriculum/The%20first%20computer%20at%20Vassar.html. Дата обращения 12.05.2022 г.

15 «История интернета: ARPANET — зарождение», автор Вячеслав Голованов, сообщество IT-специалистов «Хабр» // официальный информационный ресурс www.habr.com – URL: https://habr.com/ru/post/456200/. Дата обращения 16.10.2021 г.

16 «The First Computer Virus of Bob Thomas Explained: Everything You Need to Know», by History Computer Staff, January 4, 2021 / November 21, 2021. URL: https://history-computer.com/the-first-computer-virus-of-bob-thomas/. Дата обращения 21.03.2022 г.;

17 «Famous or Infamous? You Decide». Mitnicksecurity. GlobalGhost team TM. // Official website www.mitnicksecurity.com – URL: https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security. Дата обращения 09.05.2022 г.

18 «Информационная безопасность», автор В. А. Галатенко, Открытые системы. СУБД №04, 1995, стр. 1-5;

19 «Маркус Хесс - Markus Hess»б информационный вортал «Википедия» // официальный информационный ресурс www.wiki5.ru – URL: https://wiki5.ru/wiki/Markus_Hess. Дата обращения 24.04.2022 г.

20 «Эволюция вирусов и антивирусов. Эпохи DoS и интернет», автор А. Никишин. Информационный портал «CNews| Аналитика» // Официальный информационный ресурс www.cnews.ru – URL: https://www.cnews.ru/reviews/free/security2006/articles/evolution3/?print. Дата обращения 07.05.2022 г.

21 «The Internet Worm Program: An Analysis», author Eugene H. Spafford, Purdue Technical Report CSD-TR-823, Department of Computer Sciences Purdue University West Lafayette, 2004 – p. 23.

22 «The Yahoo Cyber Attack & What should you learn from it?"», by Elizabeth Redfern, November 4, 2021;

23 «International Cybersecurity Information Sharing Agreements», authors

Theresa Hitchens and Nilsu Goren, Published by: Center for International & Security Studies, U. Maryland;

24 Официальный информационный ресурс Международного союза электросвязи www.itu.com – URL: https://www.itu.int/en/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx. Дата обращения 23.04.2022 г.

25 Global Cyber Security Capacity Centre, 2016, p. 7;

26 Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series- No. 185.

27 «Безопасность и искусственный интеллект», BIS Journal, 31 января 2021 г. // Официальный информационный www.ib-bank.ru – URL: https://ib-bank.ru/bisjournal/news/15041. Дата обращения 24.05.2022 г.

28 Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")» // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет» – URL: https://adilet.zan.kz/rus/docs/P1700000407. Дата обращения 24.05.2022 г.

29 «Как цифровизация в Казахстане стала угрожать кибербезопасности», Маргарита Бочарова, журналист, Алматы, Казахстан, 02.02.2022 г. Central Asian Bureau for Analytical Reporting. URL: https://cabar.asia/ru/kak-tsifrovizatsiya-v-kazahstane-stala-ugrozhat-kiberbezopasnosti. Дата обращения 09.05.2022 г.;

30 «Культура защиты персональных данных: от онлайн свобод к цифровой слежке?», автор А.Гусарова, Директор Центральноазиатского института стратегических исследований (Алматы), 13.04.2020 г., Central Asian Bureau for Analytical Reporting. URL: https://cabar.asia/ru/kultura-zashhity-personalnyh-dannyh-ot-onlajn-svobod-k-tsifrovoj-slezhke. Дата обращения 09.05.2022 г.;

31 Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827 «Об утверждении Государственной программы "Цифровой Казахстан"». Утратило силу постановлением Правительства Республики Казахстан от 17 мая 2022 года № 311.

32 «Лаборатория Касперского» обновляет бизнес в Центральной Азии, 15.04.2021 г. Компания по разработке антивирусного программного обеспечения // Официальный информационный литература – URL: https://www.kaspersky.ru/about/press-releases/2021_laboratoriya-kasperskogo-obnovlyaet-biznes-v-tsentralnoi-azii-i-naznachaet-kommercheskogo-direktora. Дата обращения 11.05.2022 г.;

33 Форма отчета № 1-М «О зарегистрированных уголовных правонарушениях». Раздел 1. Сведения о зарегистрированных уголовных правонарушениях // Информационный ресурс Комитета по правовой статистике и специальным учетам – URL: https://qamqor.gov.kz/crimestat/indicators. Дата обращения 01.05.2021 г.

34 Тайна "гей-девочки из Дамаска": трагедия или подделка. 09 Июня 2011 г. Информационный, новостной портал www.URL:

https://www.newsru.co.il/mideast/09jun2011/gay_girl_103.html. Дата обращения 23.10.2021 г.

35 «Интернет статистика - 2021» Международная онлайн-школа инновационного бизнеса // официальный сайт www.moshib.su - URL: https://moshib.su/stats/internet_statistika_2021/. Дата обращения 23.10.2022 г.;

36 «Отчета о состоянии цифровой сферы Digital 2021» – UTL: https://datareportal.com/reports/digital-2021-global-overview-report. Дата обращения 04.05.2022 г.

37 «Доступный интернет: Казахстан вошёл в ТОП-10 стран мира с самым дешёвым мобильным интернетом», 05.03.2021 г. // информационный портал RANKING.KZ – URL: http://ranking.kz/ru/a/infopovody/dostupnyj-internet-kazahstan-voshyol-v-top-10-stran-mira-s-samym-deshyovym-mobilnym-internetom. Дата обращения 15.10.2021 г.;

38 «Подборка статей по кибератакам. Хроника событий» Информационный портал «Tadviser: государство, политика, технологии» // Официальный информационный ресурс www.tadiser.ru – URL: https://www.tadviser.ru/index.php/Статья:Кибератаки. Дата обращения 15.10.2021 г.

АНАЛИТИЧЕСКАЯ ЗАПИСКА

Автора проекта: Жакибеков Ержан Тукенович
Научный руководитель: Сомжүрек Баубек Жұмашұлы

Идея проекта	Уголовно-правовые аспект международных отношений в сфере кибербезопасности
Проблемная ситуация	Говоря о вопросе кибербезопасности необходимо сразу отметить, что это постгосударственная проблема и не может рассматриваться в контексте отдельно взятого государства. Google ежедневно блокирует более 18 млн. электронных писем по всему миру и это только на своих ресурсах [1]. В постпандемийный период Интернет-мошенничество возросло на 400 % [2]. Расходы на обеспечение кибербезопасности во всем мире вынуждено увеличиваются до 200 миллиардов долларов [3]. Ситуацию усугубляет активное применение информационных технологий в межгосударственных и военных конфликтах. За день до начала спецоперации России в Украине, все информационные ресурсы страны подверглись кибератаке [4]. Более того, за последние 5 лет ни одни политические выборы не проходят без вмешательства извне, в том числе с применением информационных технологий. В 2021 году Казахстан занял 31 место в Глобальном Индексе Кибербезопасности [5]. Однако по количеству межправительственных соглашений в сфере кибербезопасности Казахстан далеко отстал от развитых стран мира. Такие соглашения нужны для обмена информацией о новых типах угроз, поведения расследования кибератак, оперативного устранения нанесённого ущерба, подготовки эффективных

	отечественных специалистов. Но, как говорил хакер № 1 в мире Кевин Митник главным источником любой киберугрозы остается человек, его халатность и не осведомленность [6].
Имеющиеся решения данной проблемы	Деятельность по обеспечению информационной безопасности подкрепляется Законом «О национальной безопасности». В текущем году завершают свою реализацию две государственные программы: «Цифовой Казахстан», Концепция «Киберщит». Казахстан ратифицировал два международных соглашения касающихся кибербезопасности «Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности» и «Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий». В стране три государственных органов занимающиеся вопросами кибербезопасности. В том числе КНБ, который отвечает за национальную безопасность в киберпространстве, МВД, которое занимается расследования правонарушений, совершенных с применением информационных технологий, в соответствии с уголовным законодательством и МЦРиАП, которое в большей степени отвечает за безопасность персональных данных, хранящиеся на государственных ресурсах. Имеются отечественные разработки информационных систем безопасности (AWS CORE 2014, T&T Security). Казахстан представлен в международном сообществе по кибербезопасности (CAMP, FIRST, APCERT, OIC-CERT, APWG и др.). В основном Казахстан представлен в лице KZ-CERT (госучастие) и организаций финансового сектора (Нацбанк и тд).

	Также представлен частный сектор в лице таких организаций как ОЮЛ «ЦАРКА», Nitro Team, T&T Security. Кроме того, функционируют такие ресурсы как WebTotem и BugBounty.
Предлагаемое решение данной проблемы	1) Проработать вопрос о заключении двухсторонних межправительственных соглашений в области кибербезопасности по направлениям: - обучение/повышение квалификации; - киберпреступность, процедуры цифровой криминалистики и экстрадиции; - исследования, то есть анализ инцидентов и разработка перспективных решений (продуктов); - военные, при обнаружении признаков совершения кибератак угрожающих суверенитету государства, возможность обращаться за поддержкой кибер-войск государства-партнера; - обмен информацией и передового опыта. 2) Актуализировать уголовное законодательство, в части внесения новых составов за нарушения связанные с кибершпионажем, кибершантажом, криптомошенничеством и цифровой коррупцией, покушением на убийство по средством IT-технологий и др. 3) Постепенно переводить отечественные информационные ресурсы на продукты отечественного производства, заменяя иностранный софт. 4) Создать условия для развития научно-исследовательского потенциала. Необходимо разрабатывать собственные системы защиты, исключив какую-либо зависимость от других государств. Проекты уже имеются, необходима подержка. 5) Увеличение госзаказа на подготовку IT-специалистов.

	6) Проработать вопрос о создании мотивирующих условий для закрепления IT специалистов в стране. К примеру, льготное ипотечное кредитование. РИСКИ: 1) Несогласия с проводимой политикой главного стратегического партнера Российской Федерацией. Так как, они имеют принципиальные разногласия со многими странами по вопросам международной кибербезопасности. 2) Вмешательство стран-партнеров во внутренние дела государства. 3) При повышении уровня отечественных специалистов, увеличивается вероятность их миграции зарубеж.
Ожидаемые результаты	Полностью исключить кибератаки на информационные ресурсы Казахстана невозможно, но можно быть готовым. Соглашения об обмене информацией, позволят нашим специалистам иметь представление о новейших формах и типах кибератак, а передовой опыт способствует оперативному реагированию по предотвращению и устранению ущерба. Соглашения об обучении предоставит нашим специалистам к новейшим знаниям и практикам по кибербезопасности. Соглашения об исследованиях способствует развитию научного потенциала и разработке эффективных программных решений, самое главное отечественных. Военные соглашения обеспечат оперативную реакцию на инциденты в информационном пространстве при чрезвычайных ситуациях. Новые нормы уголовного кодекса позволят привлекать к ответственности, злоумышленников, в том числе в других странах через межправительственные соглашения. Удастся не остановить, но замедлить миграция IT-

	специалистов зарубеж.
Литература	1) «Google ежедневно блокирует миллионы фишинговых писем», автор: Владимир Фетисов, Digital Daily Digest, 18 апреля 2020 года; 2) «Эволюция мошенничества в эпоху COVID-19», автор: Гектор Родригес, журнал Плас, 14 февраля 2022 года; 3) Оценка Accenture — компания, работающая в области управленческого консалтинга, информационных технологий и аутсорсинга; 4) URL: https://www.bbc.com/russian/news-59983473; 5) URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf;