АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ МИРЕ: ОСНОВНЫЕ ПОНЯТИЯ И ТЕНДЕНЦИИ

Учебное пособие

КОСШЫ-2023

УДК 343.3/.7
ББК 67.408

Рекомендовано к изданию кафедрой специальной подготовки по противодействию глобальным угрозам Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

Рецензенты:
Бекишева С.Д. - доктор юридических наук, доцент, главный научный сотрудник Центра координации исследований и изучения проблем правоохранительной деятельности Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.
Кайназарова Д.Б. - кандидат юридических наук, доцент кафедры уголовного преследования и оперативно-розыскной деятельности Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.

Калиев А.А. – Киберпреступность в современном мире: основные понятия и тенденции. / Учебное пособие. – г. Косшы, 2023. – 103 с.

Данное учебное пособие содержит понятие киберпреступности, раскрывает основные виды киберпреступлений, способы их совершения, описывает лиц, их совершающих.

Представленный материал будет полезен как сотрудникам правоохранительных органов, занимающимся расследованием уголовных правонарушений, совершаемых с использованием информационно-коммуникационных технологий, так и студентам и преподавателям вузов, изучающим вопросы противодействия киберпреступности.

УДК 343.3/.7
ББК 67.408

ISBN

СОДЕРЖАНИЕ

Введение

Развитие современных технологий дало человечеству много различных преимуществ, связанных с эффективностью профессиональной деятельности, коммуникациями, открытиями и разработками. Главное их преимущество – они экономят наше время, позволяют совершать те или иные действия за относительно небольшое время.

Однако, несмотря на все эти положительные преимущества, научно-технический прогресс принес с собой и проблемы, с которыми столкнулись все государства мира. И эта проблема называется киберпреступность.

Осознав свою безнаказанность за уголовные правонарушения, совершаемые в киберпространстве, преступники стали больше вникать, изучать и использовать интернет как площадку для своих действий.

С каждым годом происходит рост преступлений, совершенных с использованием информационно-коммуникационных технологий и сети интернет. Те преступления, которые раньше совершались в реальном мире, стали переходить в онлайн, что обеспечивало им свободу действий и безопасность.

Киберпреступность стала настолько быстро развиваться и расширять свои горизонты, что правоохранительные органы не смогли сразу адекватно и своевременно реагировать на эти вызовы.

Сегодня киберпреступность стала одной из самых острых и глобальных проблем в мире. Она стала проникать практически во все сферы жизни человека: политику, экономику, здравоохранение.

Киберпреступники для совершения преступлений стали использовать компьютерные системы и сети, к которым им удавалось получить доступ. С их помощью они похищали информацию, наносили ущерб информационным системам и устройствам, а также нарушали права и свободы людей.

Киберпреступность включает в себя ряд различных видов преступлений, таких как хакерские атаки, вирусы и вредоносные программы, фишинг, мошенничество в интернете, кража денежных средств и личных данных, рассылка спама и многое другое.

Преступления данной категории часто сопровождаются значительными материальными убытками. Они могут иметь серьезные последствия для национальной безопасности и стабильности государства.

Поэтому борьба с киберпреступностью является одной из главных задач правоохранительных органов во всем мире.

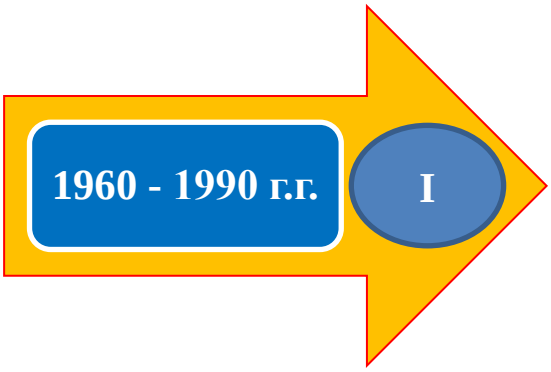
Подготовленное учебное пособие «Киберпреступность в современном мире: основные понятия и тенденции» представляет собой обзор основных аспектов и понятий, связанных с киберпреступностью. В нем рассматриваются различные виды киберпреступлений и их особенности. Автором указаны актуальные проблемные вопросы, влияющие на выявление

и раскрытие киберпреступлений, предложены меры по повышению эффективности их расследования.

Все материалы учебного пособия представлены в простой и удобной форме, доступной для восприятия. Его главной целью является получение сотрудниками правоохранительных органов, а также преподавателями и слушателями (курсантами) специализированных вузов первичных знаний о киберпреступлениях и лицах, их совершающих.

1. История зарождения и развития киберпреступности

Историю киберпреступности условно можно разделить на несколько этапов, связанных с развитием информационных технологий и интернета.



Первые упоминания о киберпреступности неразрывно связаны с началом появления и дальнейшего развития в 1960 году электронно-вычислительных машин (далее - ЭВМ). Это было уже третье поколение ЭВМ, которые стоили очень дорого, занимали огромную площадь и требовали специальную систему охлаждения.

В те времена компьютерные преступления значительно отличались от преступлений, совершаемых сегодня, и связаны были с использованием компьютера, а точнее с манипулированием компьютерными программами.

Чуть позже к числу таких преступлений стали относить и незаконные действия с телефонной линией. В 1970-ые годы популярность стало приобретать незаконное использование телефонных сетей для совершения местных и международных звонков. Такие преступления назывались «фрикингом», обозначающее взлом телефонных автоматов, телефонных сетей, а людей, их совершающих, фрикерами. Эта была особая группа людей, занимавшихся клонированием телефонных сигналов[1].

В 80-ые годы преступления уже перешли от обычных и безобидных звонков к взлому информационных систем, компьютеров, разработке вредоносных программ. В тот период появились первые хакерские журналы, а также электронные доски, ставшие площадкой для обмена информацией между лицами, занимавшимися незаконной деятельностью в сети.

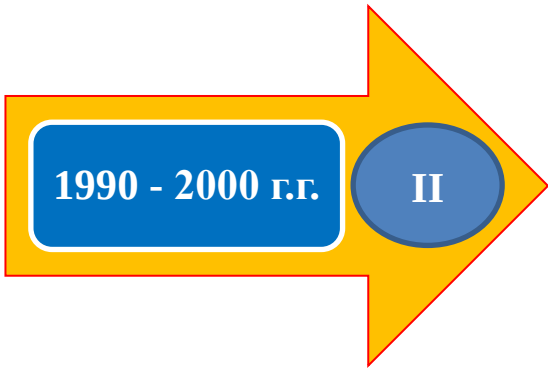
В 1988 году появилась известная во всем мире вредоносная программа – «Червь Морриса», получившая свое название от имени студента Корнельского университета США Роберта Морриса, разработавшего данный вирус, который поразил около 6000 университетских и правительственных компьютеров по всей территории Америки, причинив огромный ущерб. Это 10% от всех узлов, задействованных в работе интернета.

Червь, попадая на компьютер, делал несколько своих копий, каждая из которых замедляла его работу до тех пор, пока все системы рабочей станции не переставали отвечать.

Для борьбы с данным вирусом были задействованы самые лучшие по тем временам специалисты по компьютерным технологиям.

[1] https://www.techopedia.com/definition/4050/phreaking

Нельзя не отметить и 1983 год, когда несколько подростков, приписывающих себя к так называемой «Банде – 414», взломали компьютеры Лос-Аламосской лаборатории ядерных исследований.



Это этап развития и распространения интернета. Он дал старт для формирования новой киберпреступности. С увеличением количества пользователей всемирной паутины, происходил рост киберпреступников, которые продолжали совершенствовать свои вредоносные программы, распространяя посредством глобальной сети всемирной паутины.

С появлением интернета человечество получило возможность на расстоянии взаимодействовать между собой, учиться, работать, развлекаться, находить нужную информацию. Первый интернет был настолько прост по своей конструкции, что объединял только определенные узлы (рабочие станции), задача которых заключалась в получении и передаче информации. Работали такие системы на телефонных линиях, что создавало некоторые неудобства при соединении станций.

Следует отметить, что интернет по всему миру распространялся не равномерно, поэтому киберпреступность распространялась лишь в тех местах, где он был доступен для человека. Это вся территория Соединенных Штатов Америки, Канада, Австралия, Япония и Европа.

В этот период стали появляться новые виды вирусов, цель и функциональное назначение которых были разные. В мире киберпреступности появился новый термин «взлом». Злоумышленники, используя уязвимости информационных систем, блокировали работу отдельных устройств, похищали личные данные пользователей интернета. Тогда еще немногие задумывались об информационной безопасности своих устройств. Имя учетной записи совпадало с реальным именем человека, а пароль был самым простым или вовсе дублировал имя человека.

Распространенным видом киберпреступлений была кража кредитных карт и взлом телефонных сетей.

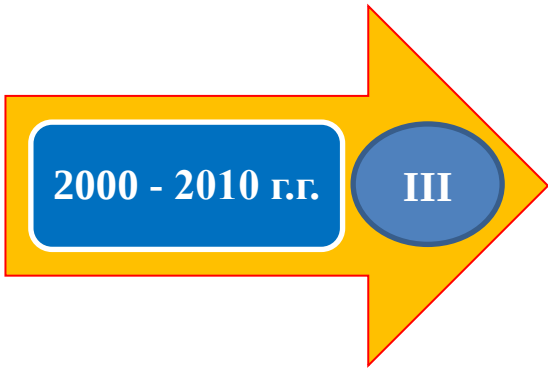
В 1993 году состоялся первый и, наверное, самый большой съезд хакеров из разных стран. В последующем такие встречи стали ежегодными. Лица, заявляющие себя хакерами, знакомились между собой, обменивались опытом, программами и технологией. Появляются специализированные форумы, где обсуждаются не только технологии и программы, используемые для незаконных действий, но и производится продажа незаконных товаров.

1995 год стал переломным периодом в мире киберпреступников. Правоохранительными органами были задержаны и в последующем осуждены знаменитые на весь мир киберпреступники – Кевин Митник и Владимир Левин.

В 1997 году хакеры разработали и запустили вредоносную программу под названием «AOHELL», от действия которой пострадали почтовые сервисы интернет провайдера.

Уже через год киберпеступники стали больше атаковать операционные системы Windows, находя в них уязвимости. Стали появляться так называемые троянские программы, которые предоставляли их создателю возможность удаленно подключаться к компьютеру, подключенному к интернету и воровать оттуда данные. Но кроме этого они могут удалять, блокировать, изменять, копировать данные, находящиеся на компьютере жертвы, нарушать работу самих компьютеров и компьютерных сетей.

Отличие троянских программ от компьютерных червей и других вирусов заключается в том, что они сами себя не воспроизводят.



Период расцвета социальных сетей и сотовых телефонов. Киберпреступники стали использовать методы социальной инженерии для получения персональных данных через социальные сети, популярные мессенджеры. Продолжались хищения денежных средств через интернет, путем незаконного проникновения в информационные системы.

Сегодня технологии далеко шагнули вперед, наравне с компьютерами стали работать сотовые телефоны, которые нисколько не уступают по производительности и функциональности. Иногда даже превосходят компьютерную технику.

В этот период произошли самые громкие киберпреступления, связанные со сбоем работы информационных систем, а также проникновением в информационные сети частных и государственных органов.

В 2001 году группа хакеров совершила кибератаку на информационную сеть Давосского форума, откуда были похищены персональные данные его участников, в том числе генерального секретаря ООН Кофи Аннана и основателя знаменитой компьютерной корпорации Microsoft Билла Гейтса[2].

В 2003 году киберпреступники атаковали несколько ведущих торговых интернет площадок в Южной Кореи, заблокировав учетные записи около 17 млн. покупателей по всему миру.

Преступление было совершено с помощью методов Dos и DDos –атак. Их суть заключается в том, чтобы перезагрузить работой целевую систему на столько, что она перестает отвечать на запросы пользователя сети.

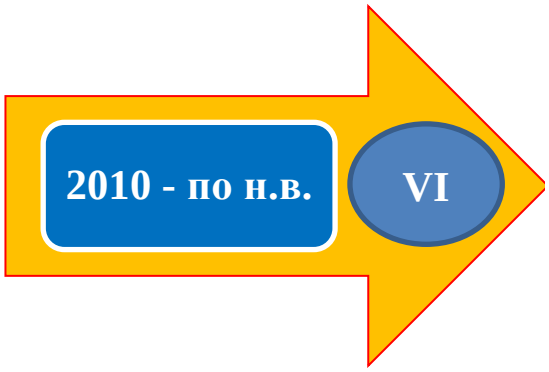
[2] https://tass.ru/info/1408961

От действия таких кибератак пострадали также знаменитые интернет сайты – «eBay», «Yahoo!», «Amazon» и многие другие.

Аналогичным методом в 2007 году были атакованы государственные сайты Президента, Парламента и Министерства иностранных дел Эстонской Республики.

Еще одно крупное киберпресутпление произошло в апреле 2009 года, когда преступники из информационной системы Пентагона похитили информацию об одном из военных самолетов США.

Чуть позже в июле 2009 года киберпреступники повторили сценарий Эстонии, атаковав важные государственные сайты Южной Кореи (главы государства, правительства и других важных государственных органов).



Это этап профессионального роста кибер - преступников. Стали использоваться сложные с технической стороны методы совершения преступлений. Преступники стали использовать современные технологии и собственные разработки в своих целях, такие, например, как искусственный интеллект и криптовалюты, которые обеспечивали им анонимность.

Конечно, по сравнению с прошлыми годами уровень профессиональных навыков киберпреступников значительно вырос. Сама преступность стала более организованной.

С развитием электронной коммерции и банковских операций в интернете, киберпреступники также стали совершенствовать свои методы атак. Больше стало использоваться хищение личных данных и финансовых ресурсов через фишинговые атаки и кардинг (вид мошенничества с платежными картами).

Отдельные киберпреступники и группы внутри страны или со всего мира стали создавать целые сообщества, объединяющие разработчиков вредоносных программ, дроповодов, дропов, хакеров, и других узких специалистов в единую преступную сеть.

В последние годы, с развитием новых технологий, таких как блокчейн, искусственный интеллект и Интернет вещей, киберпреступники стали использовать их в своих преступных целях.

Поменялось направление кибератак, они больше стали нацелены на умные дома, устройства Интернет вещей и криптовалютные биржи.

Самым большим вызовом для борьбы с киберпреступностью является постоянное развитие технологий и появление новых видов кибератак.

Преступники постоянно находят и используют новые способы незаконного проникновения в информационные и компьютерные системы и сети, мошенничества и хищения данных.

В настоящее время киберпреступность является всемирной проблемой, требующей глобального взаимодействия и международного сотрудничества, в том числе по обмену информацией, разработке законодательных актов и совместным мероприятиям, направленным на предотвращение и пресечение киберпреступлений.

Вопросы для самоконтроля:

1) Как называется незаконное использование телефонных сетей для совершения звонков?

2) Кто такие фрикеры?

3) С чем связан второй этап зарождения и развития киберпреступности?

4) Чем характеризуется третий этап зарождения и развития киберпреступности?

2. Киберпреступления и киберпреступники

1.1. Понятие киберпреступление?

В современном цифровом веке, информационные и коммуникационные технологии стали неотъемлемой частью нашей повседневной жизни. Однако за этими технологическими прорывами стоят и новые угрозы, которые можно обобщить под термином «киберпреступность».

Начнем с определения киберпреступности. Что же такое киберпреступление? Если сказать простыми словами - это форма преступности, которая использует компьютеры, сети и электронные устройства для осуществления незаконных действий. Киберпреступники при совершении своих незаконных действий применяют различные схемы и техники, чтобы получить доступ к конфиденциальной информации, финансовым данным или нарушить работу компьютерных систем.

На самом деле существует множество различных определений, описывающих процесс их совершения. Одни специалисты в области информационной безопасности считают, что это преступления, совершаемые с помощью интернета, другие, предлагают относить к этой категории и преступления, совершаемые против компьютерной системы и сети.

Автором данного учебного пособия предложено следующее определение киберпреступности, объединяющее разные формулировки.

Преступления, совершаемые с использованием информационно - коммуникационных технологий (киберпреступления), – это действия пользователя компьютерной системы, мобильной сети (сотовой связи), в том числе посредством сети интернет, против компьютерной системы, сети и данных, а также с помощью компьютерной системы, сети и данных.

Киберпреступность стала беспрецедентным вызовом для общества и экономики. Рост числа кибератак и киберпреступлений связан с быстрым развитием информационных технологий и все большей зависимостью людей и организаций от цифровых ресурсов.

По мнению руководителя Российской Ассоциации Электронных Коммуникаций С.Плуготаренко, в разных точках земного шара работают около 40 миллионов киберпреступников, ущерб от действий которых оценивается в 500 миллиардов долларов. При этом количество вирусных атак в мире растёт по 3 процента в месяц, атак на веб-сервисы - по 2,5 процента, а число краж денег с различных устройств или электронных кошельков - по 3,5 процента[3].

[3] Российская Ассоциация Электронных Коммуникаций (РАЭК). «Глобальные киберугрозы: возможно ли безопасное развитие цифровой инфраструктуры?»// (http://raec.ru/live/raec-news/9471/) – интернет - источники

Более того, несмотря на постоянный рост киберпреступлений, раскрываемость их по-прежнему остается очень низкой.

Так, по мнению специалиста по кибернетике и системе управления, автора многих публикаций в области развития информационно-коммуникационных технологий В.П. Филимонова, раскрываемость киберпреступлений в мире составляет не более 3-4%[4].

Главными причинами роста и распространения киберпреступности являются увеличение количества пользователей интернета, безнаказанность, анонимность, безопасность и легкость заработка.

Увеличение количества пользователей интернетом.

Риск распространения вредоносных программ (т.н. вирусов) возрастает с увеличением количества пользователей всемирной паутины, большинство из которых не знают или не придают особого значения защите своих персональных данных, находящихся в персональных компьютерах, ноутбуках, смартфонах или планшетах.

По последним данным ITU и GSMA Intelligence, количество пользователей интернета в мире по состоянию на текущий год составляет 5,16 миллиарда[5].

Этот факт признает один из ведущих экспертов в области информационной безопасности Евгений Касперский, называя рост числа пользователей интернета одной из главных причин, влияющих на рост киберпреступности.

По данным международного агентства We Are Social, опубликованном в отчете Global Digital, в мире насчитывается более 4-х миллиардов пользователей сети интернет, что соответствует 52 процентам всего населения мира[6].

Ожидается, что с каждым годом эта цифра будет только расти.

Приобретая компьютер и подключаясь к сети интернет, граждане не задумываются о своей безопасности, кибергигиене. Даже если кто и пользуется антивирусом, он не всегда уделяет внимание обновлению антивирусной базы.

Тем самым, каждый такой пользователь становится мишенью в руках киберпреступников.

---

[4] Филимонов, В.П. Киберпреступность уже засшкаливает!/ В.П.Филимонов // Русская народная линия, информационно-аналитическая служба //(http://ruskline.ru/special_opinion/2017/fevral/kiberprestupnost_uzhe_zashkalivaet/) – интернет-источники.

[5] https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/#:~:text=%D0%9F%D0%BE%20%D0%BF%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BD%D0%B8%D0%BC%20%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%BC%20ITU%20%D0%B8,%D0%BB%D0%B8%D1%88%D1%8C%20%D0%BD%D0%B0%2098%20%D0%BC%D0%B8%D0%BB%D0%BB%D0%B8%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D0%B5%D0%B9

[6] (http://www.bizhit.ru/index/polzovateli_interneta_v_mire/0-404) – интернет-источники.

Безнаказанность.

Она характеризуется отсутствием для преступника каких-либо негативных последствий. Современные киберпреступники стараются выбирать местом совершения преступлений преимущественно те точки земного шара, где, во-первых, менее развита нормативно-правовая база, во-вторых, широко используются новые технологии и сеть интернет.

Там, где нет соответствующей нормативно-правовой базы, органы правопорядка не могут привлекать виновных лиц к ответственности.

Анонимность.

Стала третьей по значимости причиной роста и распространения киберпреступности. Большая часть пользователей всемирной паутины во всем мире предпочитают оставаться анонимными. Такой подход к работе в интернете связан с рядом причин, в том числе незаконной деятельностью, выходящей за рамки правового поля.

Безопасность.

Отсутствие систем информационной защиты или недостаточная их работоспособность, а также различные уязвимости в программном обеспечении подталкивали определенную группу людей, вовлеченных в среду развития IT-технологий, проникнуть в компьютерную систему, причиняя порой материальный ущерб ее владельцу.

При этом риск быть пойманным на месте совершения преступления для киберпреступника был минимальным или вообще отсутствовал в виду нахождения правонарушителя далеко от потерпевшего. Их могут разделять не просто города. В большинстве случаев такие преступления совершаются лицами, находящимися в другой стране.

Легкость заработка.

Данная причина роста киберпреступности стала движущей силой по привлечению людей в преступную среду. Еще в начале 2010 года об этом заявлял один из руководителей антивирусной компании Касперский. На сегодняшний день киберпреступность является хорошо организованным преступным бизнесом.

В настоящее время правоохранительные органы всего мира отмечают появление новых видов киберпреступлений, которые с каждым днём только совершенствуются.

Вопросы для самоконтроля:

1)Что такое киберпреступление?

2)Назовите причины роста и распространения киберпреступлений.

3)Чем характеризуется безнаказанность киберпреступления?

4) Назовите причинную связь между увеличением количества пользователей интернета и ростом киберпреступлений?

1.2. Кто такие киберпреступники?

Киберпреступления совершают лица, именуемые в научной литературе киберпреступниками. Они подразделяются на хакеров, фрикеров, крэкеров, кардеров, вирусописателей, скамеров, спамеров и т.д.

Автором данного учебного пособия предложено следующее определение термину «киберпреступник».

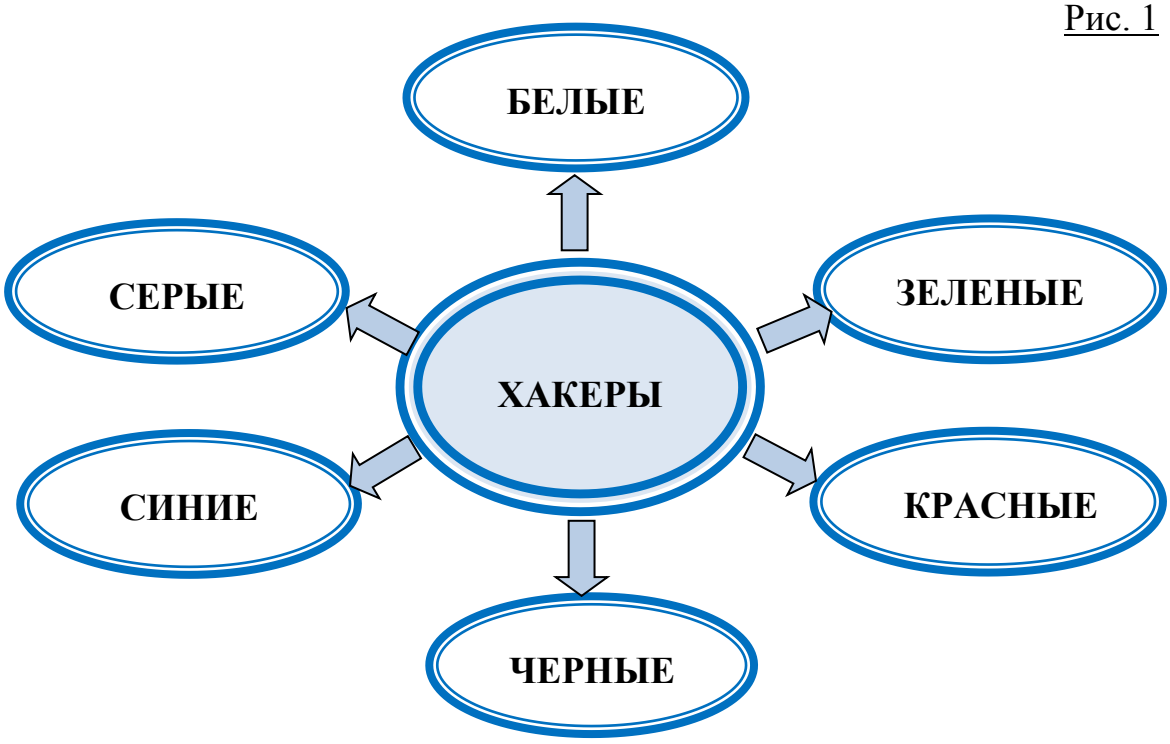
Киберпреступник – это человек, который использует свои знания и современные технологии для совершения уголовных правонарушений с целью получения материальной выгоды или без таковой. Для совершения таких преступлений, он может не обладать знаниями в области IT – технологий, но при этом воздействовать на устройство, системы, сети и хранящиеся в них данные.

Из этого определения следует, что всех кто хоть как-то использует современные устройства, информационно-коммуникационные технологии, компьютерные программы, системы, сети, а также информацию, которую они хранят и обрабатывают в незаконных целях можно отнести к категории «киберпреступник».

В различных интернет - источниках термин «хакер» ассоциируется с понятием преступник. На самом деле данный термин применяется не только к компьютерным преступникам, но и к любым специалистам в области компьютерных систем и программ. Например, IT-специалиста (администратора сети), настраивающего сеть или систему, а также находящего в ней уязвимости тоже можно назвать хакером.

Хакеры подразделяются на несколько видов:

Рис. 1



Белыми (этичными) хакерами называют IT-специалистов, тестирующих различные информационные системы на уязвимость. Их главная задача - это обнаружить и устранить проблемы информационной безопасности в информационной системе и сети.

Черными хакерами называют IT-специалистов, умышленно взламывающих различные программы, информационные системы, с целью получения материальной выгоды. Например, они проникают в системы и сети, чтобы похитить конфиденциальные данные или загрузить в систему вредоносное программное обеспечение.

Серыми хакерами называют IT-специалистов, которые проникают в систему, тестируют ее на уязвимость с целью получения оплаты от владельца данной системы за устранение проблем с информационной безопасностью.

Зелеными хакерами называют молодых, еще не опытных IT-специалистов, которые только учатся проникать в системы, тестировать их на уязвимости.

Красными хакерами называют IT-специалистов, которые также как и этичные хакеры борются с проблемами информационной безопасности в системе и сети, однако применяют незаконные способы взлома.

Синими хакерами называют IT-специалистов, совершающих незаконные действия, связанные с взломом информационной системы, сети, какого-либо устройства из-за мести.

Помимо хакеров в преступной организации также могут быть следующие участники [7]:

Фрикеры (Phreacker) – злоумышленники, специализирующиеся на совершении преступлений в области электросвязи, с использованием конфиденциальной компьютерной информации и специальных технических средств, разработанных (приспособленных, запрограммированных) для негласного получения (модификации, блокирования) информации с технических каналов электросвязи.

Крэкеры (Cracker) – злоумышленники, осуществляющие «взлом» (модификацию, блокирование, уничтожение) средств защиты компьютерной информации. Основной вид их деятельности – это оборот контрафактной продукции, незаконное распространение охраняемой законом компьютерной информации.

Вирусописатели – злоумышленники, имеющие соответствующее образование или знания по созданию вредоносного программного обеспечения, для использования в совершении преступлений или без такового.

[7] http://www.cprspb.ru/bibl/forein/21.htm

Кардеры (Carder) – злоумышленники, специализирующиеся на незаконной деятельности в сфере оборота пластиковых карт.

Скамеры (Scamer) – злоумышленники, которые занимаются получением, сбором личных сведений о пользователях сети интернет, с целью их использования в корыстных целях (например, получение денежных средств, подарков и т.д.).

Спамеры (Spamer) – злоумышленники, которые занимаются массовой рассылкой по электронной почте корреспонденции лицам, нежелающим ее получать.

Киберпреступников можно также разделить на 2 категории:

Зарегистрированные (санкционированные) пользователи ЭВМ, системы ЭВМ или их сети – это лица, которые на законном основании (в силу договора, контракта) использовали ЭВМ, систему ЭВМ или их сеть для совершения компьютерного преступления.	Незарегистрированные (несанкционированные) пользователи ЭВМ, системы ЭВМ или их сети – это лица, совершившие компьютерные преступления путем несанкционированного доступа и использования чужих ЭВМ, системы ЭВМ или их сети.

Киберпреступниками могут быть также и не профессиональные IT-специалисты, простые граждане, которые знают, как использовать вредоносное программное обеспечение и применяют свои знания для совершения преступления, цель которого получить материальную выгоду или просто месть.

Например, уволили сотрудника из какой-нибудь компании, а он из-за мести зашел в рабочий компьютер и уничтожил все данные или заразил компьютерную сеть вирусом.

Киберпреступления могут совершаться как одним человеком, так и группой лиц, объединившихся для совершения преступления, с использованием информационно-коммуникационных технологий и сеть интернет.

Современные преступные сообщества давно осознали возможности интернета и его положительные стороны. Многие киберпреступники объединяются в организованные группы, иногда даже трансграничные, где каждый имеет и выполняет свою роль.

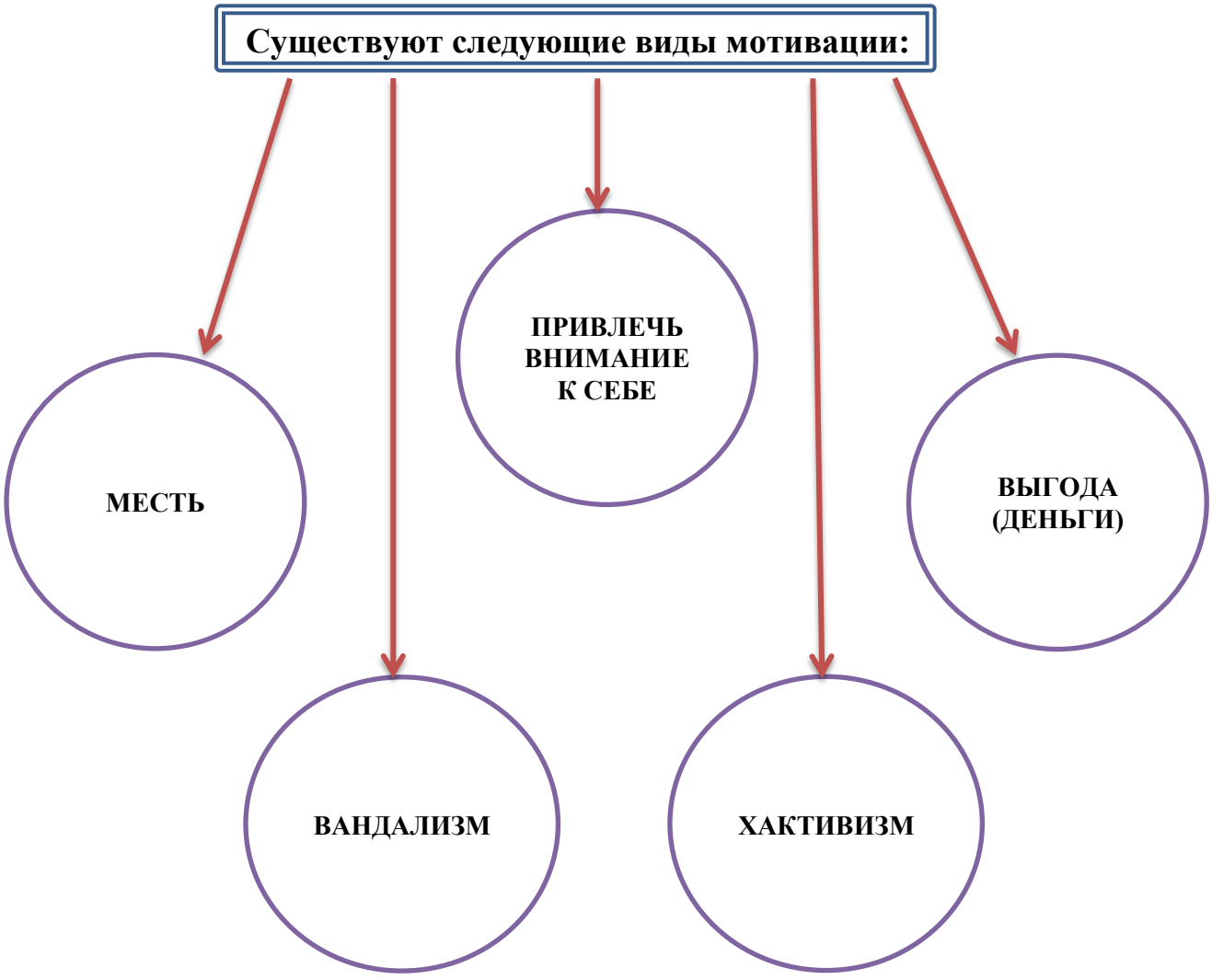
Сейчас не обязательно держать в штате хакера для совершения уголовных правонарушений. Их можно найти на специальных закрытых форумах и использовать для конкретного вида преступления, в том числе при совершении заказного убийства.

На закрытых площадках «Даркнета» можно найти форумы черных хакеров, предлагающих свои услуги и выставляющих свои достижения в области взлома информационных систем.

Обычно там происходит обмен стратегиями и инструментами, продают и покупают украденную информацию, находят работу и соисполнителей для ее выполнения.

Для чего хакеры совершают кибератаки?

Рис. 2



- желание привлечь к себе внимание – данный вид мотивации порождает ненаправленные атаки, т. е. взлом выполняется ради развлечения и не связан с определенной системой;
- материальная выгода – данный вид мотивации предусматривает уже направленные атаки, целью которых является получение конкретной

информации или доступ к конкретной системе ради получения денег или другой выгоды;

- месть – это вид мотивации, при которой кибератаки происходят с целью причинения вреда конкретному лицу или организации;
- хактивизм (hactivism) - еще одна форма мотивации, когда кибератаки связывают с политическими акциями. Такие атаки является более опасными, поскольку привлекают честных и наивных людей;
- вандализм - последней вид мотивации, при которой действия хакера имеют злой умысел. В этом случае хакер не заботится о захвате управления системой *(только если это не помогает ему в его целях)*. Вместо этого он старается причинить вред легальным пользователям, препятствуя их работе в системе, или законным владельцам сайта, изменяя его веб-страницы.

Рис. 3

Хакерские атаки условно можно поделить на 3 категории:

Относительно безобидные - к ним можно отнести те атаки, которые не наносят ущерба компьютерному оборудованию и системам. Как правило, подобные действия осуществляются с целью внедрения в компьютерные системы шпионских программ, основная цель которых заключается в сборе конфиденциальной информации. Подобные программы никак себя не обнаруживают и не влияют на работу компьютеров. По сути, владелец компьютера может долгое время работать, не подозревая, что все его личные данные утекают к хакеру.

Злонамеренные - к ним можно отнести те кибератаки, которые явно нацелены на внесение осложнений в работу отдельных компьютеров или целых сетей. Внедренное вредоносное программное обеспечение, будет саботировать работу компьютера: уничтожать или шифровать данные, ломать операционную систему, выключать или перезагружать ПК. Конечным результатом подобных действий может быть потеря времени и доходов многих компаний, нарушение доставки товаров и услуг клиентам и тому подобные последствия.

Кибертерроризм - является самым опасным среди всех разновидностей хакерских атак, так как целями нападения избираются различные важные государственные и коммунальные структуры типа энергоснабжения или транспортного сообщения. Успешно проведенная кибератака на ключевые точки инфраструктуры, может запросто парализовать страну на некоторое время, нанеся колоссальные убытки.

Кибератаки могут совершаться как отдельными правонарушителями (хакерами), так и группой или организацией, преследующих свои цели.

Ниже приведены примеры некоторых кибератак, которые можно отнести как к безобидным, так и злонамеренным.

- Использование вредоносного программного обеспечения
- Dos / Ddos – атаки и фишинг
- Атаки путем внедрения SQL кода
- Применение межсайтовых сценариев
- Использование программ – шпионов и «шантажистов»
- Организация ботнетов

Выбор кибератаки, а также их количество всегда определяется преступником самостоятельно с учетом поставленной цели и задачи. Более подробная информация о кибератаках изложена во втором разделе данного учебного пособия.

Вопросы для самоконтроля:

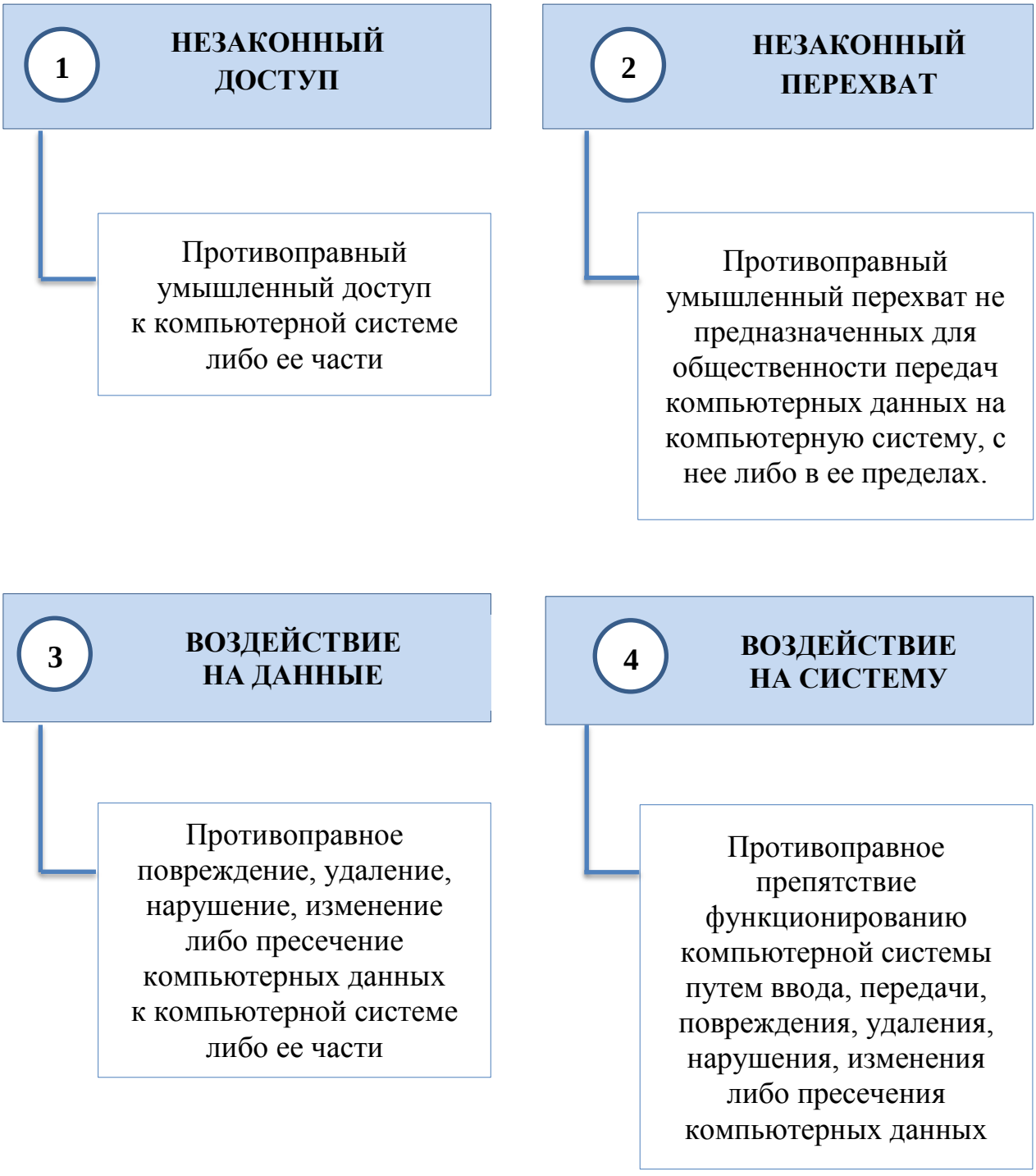
1) Кто такой киберпреступник?
2) Назовите виды хакеров.
3) Дайте определение белым и черным хакерам.
4) Назовите виды мотивации совершения кибератак.
5) На какие категории подразделяются хакерские атаки?

3. Классификация киберпреступлений, их основная характеристика, методы и способы совершения

Существуют различные виды киберпреступлений, которые отличаются между собой по способу, времени, территории их совершения, направленности действий (цели), масштабу последствий.

Конвенция Совета Европы все виды киберпреступлений подразделяет на 4 основные группы:

1) Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем.



2) Правонарушения, непосредственно связанные с использованием компьютерных средств, подключенных или неподключенных к сети интернет.

1 ПОДЛОГ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

ввод, изменение, удаление или блокирование компьютерных данных, влекущих за собой нарушение аутентичности данных

2 МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

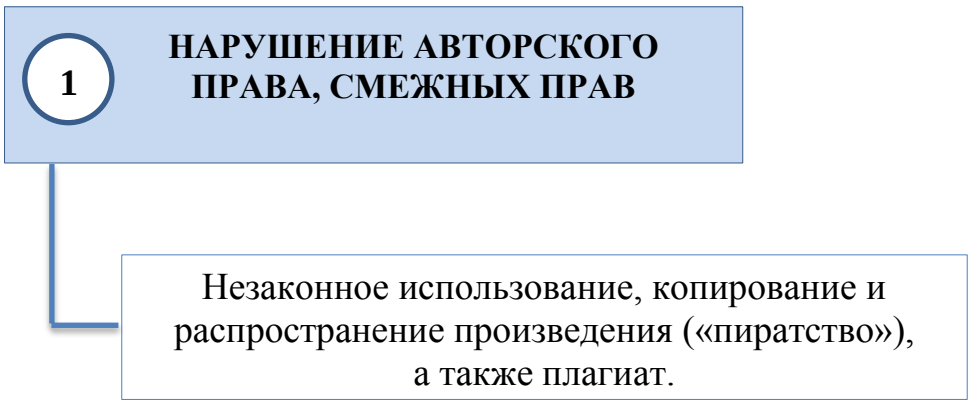
лишение другого лица собственности посредством любого ввода, изменения, удаления или блокирования компьютерных данных, а также любого вмешательства в функционирование компьютерной системы с намерением неправомерного извлечения экономической выгоды для себя или для третьих лиц.

3) Преступления, связанные с содержанием контента.

1 ДЕТСКАЯ ПОРНОГРАФИЯ

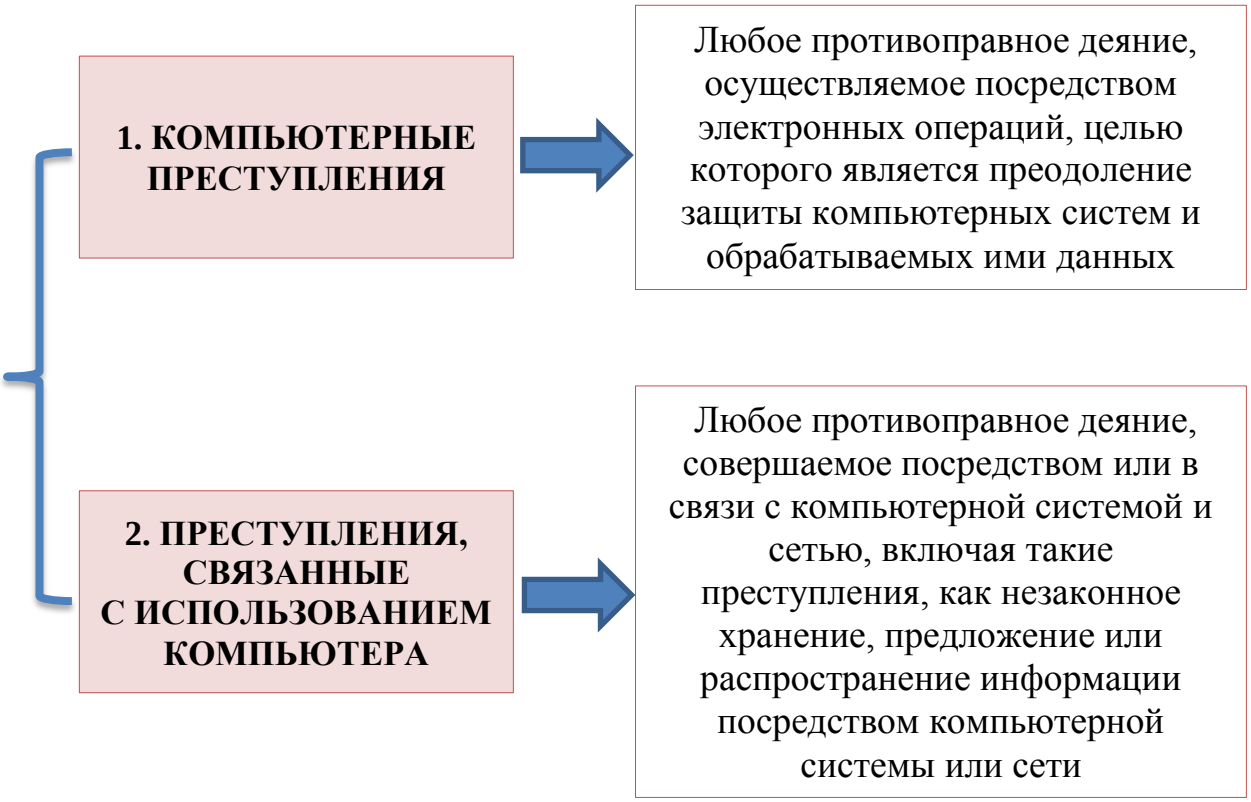
1. Производство детской порнографии в целях распространения через компьютерную систему;
2. Предложение или предоставление в пользование детской порнографии через компьютерную систему;
3. Распространение или передача детской порнографии через компьютерную систему;
4. Приобретение детской порнографии через компьютерную систему для себя или другого лица;
5. Владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

4) Правонарушения, связанные с нарушением авторского права и смежных прав.



Смежные права – права исполнителей, производителей фонограмм и организаций радио- и телевещания. Они являются смежными по отношению к авторским правам[8].

Организация Объединенных Наций по предупреждению преступности и обращению с правонарушителями, при обсуждении преступлений, связанных с использованием компьютерной сети в г. Вена, 10-17 апреля 2000 года разделила все виды киберпреступлений на 2 категории:



[8] https://www.gov.kz/memleket/entities/adilet-akm/press/article/details/103746?lang=ru

Существует и другая классификация киберпреступлений, связанная со способом их совершения, наличием или отсутствием насилия и с размером причиненного вреда.

Первая категория киберпреступлений предусматривает использование компьютера или сети в совершении уголовных правонарушений:

- *компьютер является объектом правонарушения, когда цель преступника - похитить информацию или нанести вред интересующей его системе;*
- *компьютер используется как средство, способствующее совершению преступления. Например, неправомерный доступ в информационную систему или мошенничество, совершаемое с помощью компьютерных технологий;*
- *компьютер используется как запоминающее устройство.*

Вторая категория киберпреступлений представляет собой физическую опасность человеку или группе лиц. Они могут быть:

а) насильственные:

- *кибертерроризм;*
- *угроза физической расправы через сеть интернет;*
- *детская порнография.*

б) ненасильственные:

- *хищение с использованием информационных технологий (кража, мошенничество);*

- противоправное нарушение владения в киберпространстве (правонарушители проникают в защищенную систему, не повреждая и не используя данные хранящиеся в ней; обычно киберпреступники это делают для демонстрации своих возможностей перед другими);

- разрушение (незаконное проникновение в информационную систему или сеть, удаление там программ или данных, «взлом» Web-сервера и уничтожение на нем Web-страниц, заражение вредоносными программами для блокирования системы).

Третья категория киберпреступлений определяет размер нанесенного вреда:

а) существенный вред (преступления, сопряженные с насилием против человека, причинившие значительный материальный ущерб);

б) несущественный вред (преступления, которые привели к незначительным потерям, в том числе материальным).

Согласно Уголовному кодексу Республики Казахстан, все преступления, совершаемые в киберпространстве, а также с использованием информационно-коммуникационных технологий условно можно разделить на 5 основных видов:

1	**Уголовные правонарушения против компьютерной системы:**
	• *Неправомерный доступ в информационную систему или сеть телекоммуникаций.* • *Нарушение работы информационной системы или сетей телекоммуникаций.*

2	**Уголовные правонарушения против компьютерной информации:**
	• *Неправомерный доступ к информации.* • *Неправомерные уничтожение или модификация информации.* • *Неправомерное завладение информацией.* • *Принуждение к передаче информации.*

3	**Создание и использование вредоносных программ:**
	• *Создание, использование или распространение вредоносных компьютерных программ и программных продуктов.* • *Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства.*

4	**Хищения с использованием ИКТ:**
	• *Кража, совершенная путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.* • *Мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы.*

5	**Уголовные правонарушения, связанные с незаконным контентом:**
	• *Неправомерное распространение электронных информационных ресурсов ограниченного доступа.* • *Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели.*

Рассмотрим каждую из представленных групп киберпреступлений в отдельности.

I группа: Уголовные правонарушения против компьютерной системы.

Данная категория правонарушений состоит из 2-х составов: *«Неправомерного доступа в информационную систему или сеть телекоммуникаций» (ст. 205 УК РК) и «Нарушение работы информационной системы или сетей телекоммуникаций» (ст. 207 УК РК).*

В соответствии с пунктом 12 статьи 1 Закона Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК, информационная система – это организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач[9].

Общественная опасность рассматриваемых в данном разделе уголовных правонарушений заключается в том, что они нарушают права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере, наносят вред конфиденциальности, целостности, сохранности и доступности информационных ресурсов, информационных систем и инфраструктуры связи.

[9] Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК

Объектом уголовных правонарушений, предусмотренных статьей 205 УК РК, являются права и законные интересы граждан и организаций на конфиденциальность информационных систем и сетей.

Объектом уголовных правонарушений, предусмотренных статьей 207 УК РК, являются права и законные интересы граждан и организаций на пользование информационными системами и сетями.

Предметом являются информация, информационные системы, сети телекоммуникации.

Объективная сторона данной категории правонарушений выражается в форме действия или бездействия, направленного на нарушение работы информационной системы или сетей телекоммуникаций, или в неправомерном доступе к охраняемой законом информации, содержащейся на электронном носителе, в информационной системе или сети.

Субъективная сторона уголовных правонарушений предполагает только умышленную форму вины.

Субъектом будут являться лица, достигшие 16 лет.

Деяния, предусмотренные частями 1 и 2 статьи 205 Уголовного кодекса Республики Казахстан, относятся к уголовным проступкам.

Деяния, предусмотренные частью 3 статьи 205 Уголовного кодекса Республики Казахстан, относится к преступлениям небольшой тяжести.

Деяние, предусмотренное частью 1 статьи 207 Уголовного кодекса Республики Казахстан, относится к преступлениям небольшой тяжести.

Деяние, предусмотренное частью 2 статьи 207 Уголовного кодекса Республики Казахстан, относится к преступлениям средней тяжести.

Для совершения данных видов уголовных правонарушений, преступники применяют различные виды кибератак.

Хищение цифровой личности – это вид преступления, представляющий собой незаконное завладение учетной записью пользователя сети интернет для совершения мошенничества.

Учетная запись – совокупность сведений о пользователе, необходимая для его идентификации и предоставления доступа к личным данным и системным настройкам.

Киберпреступник, используя цифровую личность человека (логин / пароль), проникает в информационную систему потерпевшего и совершает действия от его имени. При этом, целью киберпреступника могут быть как деньги, так и просто кража личных данных, семейной, медицинской, налоговой и коммерческой тайны.

Например, получив доступ к учетной записи интернет – пользователя, злоумышленник может оформить кредит в банке или другой финансовой организации, уничтожить важные данные, хранящиеся в системе или продать эту информацию.

Для совершения данного вида преступления, используются различные способы. От социальной инженерии до использования вредоносного программного обеспечения.

Иногда пользователи сами допускают утечку информации о своей учетной записи, выкладывая конфиденциальную информацию о себе в интернет, что способствует взлому используемых ими информационных систем. Устанавливают ненадежные пароли или загружают с интернета программы или документы, зараженные вирусами.

Не исключается и физический доступ к носителям информации, содержащей конфиденциальные сведения, в том числе банковские данные. Злоумышленник может работать вместе с потерпевшим в одной организации, где похитить в конце рабочего дня жесткий диск, произвести его копирование и вернуть его на место так, что потерпевший даже не догадается ни о чем. Либо поработать на компьютере потерпевшего в его отсутствии, найти нужные сведения и скопировать их. Можно также просто загрузить на компьютер потерпевшего вредоносное программное обеспечение для дальнейшей работы с устройством.

Опасность данного вида преступления заключается в том, что учетные данные пользователя сети интернет могут использовать для совершения других преступлений. Например, для совершения кибератаки на государственные и частные веб-ресурсы, отмывание денег, путем использования банковского счета потерпевшего при обналичивании денег.

По сведениям специализированных подразделений Министерства внутренних дел Республики Казахстан, граждане при краже учетных данных не воспринимают это деяние как преступление и в большинстве случаев не сообщают об этом в правоохранительные органы, ограничившись созданием новой учетной записи в информационной системе.

DoS и DDoS атаки – это вид кибератаки, целью которых является нарушение работы сайта или сервера *(например, заполнения сервера пакетами TCP и UDP)*. То есть, на требуемый сайт или сервер одновременно отправляется огромное количество запросов из одного или нескольких источников, в результате чего они временно выходят из строя *(становятся недоступными для пользователей Интернета)*.

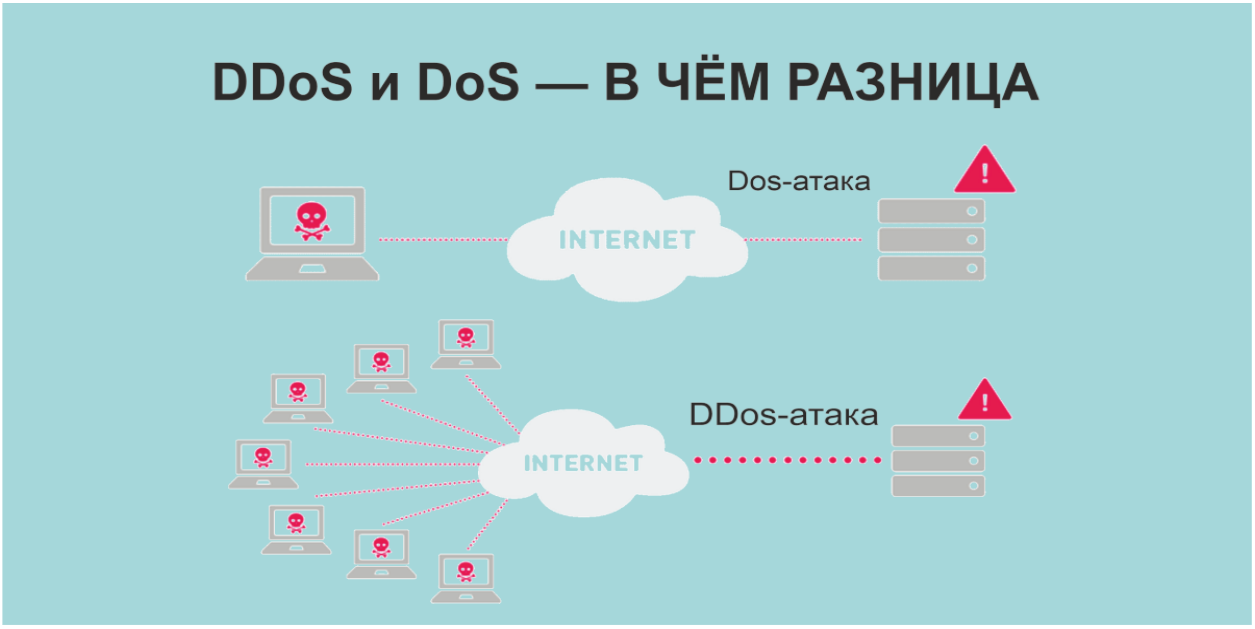
Иногда для проведения успешной кибератаки, преступники создают и используют ботнеты *(большие сети из устройств пользователей, зараженных вредоносными программами)*.

По данным Государственной технической службы КНБ РК *(далее - ГТС)*, казахстанский сегмент интернета постоянно подвергается кибератакам, основной целью которых является нарушение работы инфраструктуры Казнета.

Для минимизации угроз ГТС проводятся работы по анализу всего сетевого трафика в режиме реального времени, проверяется каждый пакет[10].

Отличие DoS и DDoS атак между собой представлено на рис. ниже.

Рис. 4



Вопросы для самоконтроля:

1) *Дайте характеристику уголовным правонарушениям против компьютерной системы.*
2) *Что будет являться объектом данных уголовных правонарушений?*
3) *Дайте определение хищению цифровой личности?*
4) *Что такое учетная запись?*
5) *Дайте определение DoS и DDoS атаки?*
6) *Назовите отличие между DoS и DDoS атаками?*

[10] https://tengrinews.kz/kazakhstan_news/otrajeno-20-millionov-atak-na-kaznet-gts-479742/

II группа: Уголовные правонарушения против компьютерной информации.

Данная категория правонарушений включает в себя уже 4 состава: *«Неправомерный доступ к информации», «Неправомерные уничтожение или модификация информации», «Неправомерное завладение информацией» и «Принуждение к передаче информации».*

Объектом уголовного правонарушения, предусмотренного частью 1 статьи 205 УК РК, являются права и законные интересы граждан и организаций на конфиденциальность информации.

Объектом уголовного правонарушения, предусмотренного статьей 206 УК РК, являются права и законные интересы граждан и организаций на целостность, сохранность и достоверность личной информации и информации в информационных системах и сетях.

Объектом уголовного правонарушения, предусмотренного статьей 208 УК РК, являются права и законные интересы граждан и организаций на конфиденциальность личной информации и информации в информационных системах и сетях.

Предметом служат информация, электронный носитель.

Объективная сторона выражается в форме действия, направленного на неправомерный доступ к информации, ее завладению, уничтожение или модификацию, принуждение к передаче информации.

Неправомерность имеет место при отсутствии разрешения собственника или владельца информации на ее копирование или владение ею, уничтожение или модификацию.

Субъективная сторона предполагает только умышленную форму вины.

Субъектом будут являться лица, достигшие 16 лет.

Деяние, предусмотренное частью 1 статьи 206 Уголовного кодекса Республики Казахстан, относится к уголовным проступкам.

Деяние, предусмотренное частью 2 статьи 206 Уголовного кодекса Республики Казахстан, относится к преступлениям небольшой тяжести.

Деяние, предусмотренное частью 3 статьи 206 Уголовного кодекса Республики Казахстан, относится к тяжким преступлениям.

Вопросы для самоконтроля:

1) Дайте характеристику уголовным правонарушениям против компьютерной информации.

2) Что будет являться объектом данных уголовных правонарушений?

3) Дайте определение целостности информации.

4) Что такое информационная система?

III группа: Создание и использование вредоносных программ.

Это особая категория правонарушений, связанных с созданием, использованием и распространением различного вредоносного программного обеспечения.

Особенность таких уголовных правонарушений заключается в том, что они могут совершаться как самостоятельно, так и в совокупности с другими преступлениями.

Например, для совершения хищения (денег, цифровой личности, аккаунтов) используются вредоносные компьютерные программы или программные продукты.

Также вредоносное программное обеспечение (далее - ВПО) используется и для неправомерного изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента.

Общественная опасность анализируемого преступления определяется масштабностью и значительностью ущерба, который может причинить вредоносная программа.

Объектом данной категории уголовных правонарушений будут выступать общественные отношения, связанные с обеспечением конфиденциальности, целостности и доступности охраняемой законом информации.

Предметами служат: абонентское устройство сотовой связи, устройство идентификации абонента, дубликат карты идентификации абонента сотовой связи, программы для изменения идентификационного кода абонентского устройства.

Абонентское устройство – средство связи индивидуального использования, формирующее сигналы электрической связи для передачи или приема заданной абонентом информации и подключаемое к сети оператора связи. Устройство идентификации абонента есть такое устройство, с помощью которого осуществляется отождествление абонента. Идентификационный код – код абонентского устройства или абонентской станции, присваиваемый заводом-изготовителем, который передается в сеть оператора связи при подключении к ней этого устройства[11].

Объективная сторона данной категории уголовных правонарушений выражается в форме действия, направленного:

- на создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, а равно умышленные использование и (или) распространение такой программы или программного продукта;

[11] Закон Республики Казахстан «О связи» от 5 июля 2004 года № 567

- на внесение вредоносных изменений в существующую компьютерную программу или программный продукт;

- на использование, распространение вредоносной компьютерной программы или программного продукта.

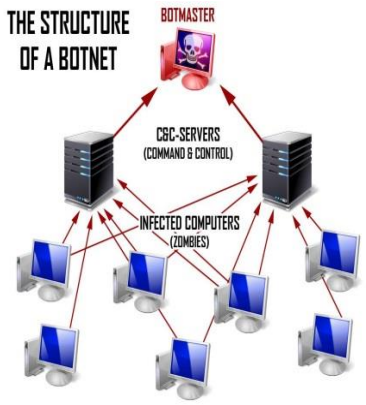
Субъективная сторона характеризуется только прямым умыслом.

Субъектом будут являться лица, достигшие 16 лет.

Деяние, предусмотренное частью 1 статьи 210 Уголовного кодекса Республики Казахстан, относится к преступлениям средней тяжести.

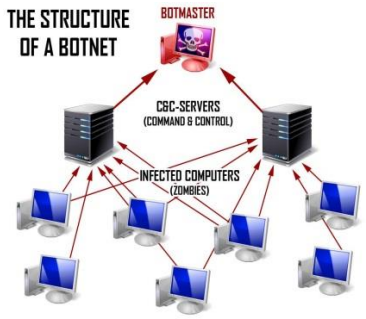
Деяния, предусмотренные частями 2 и 3 статьи 210 Уголовного кодекса Республики Казахстан, относится к тяжким преступлениям.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



Ботнеты – это компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами, которые устанавливаются скрытно на устройство жертвы и позволяют злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Они могут состоять из вирусов брандмауэров, программ для удаленного управления компьютером, а также инструментов для скрытия от операционной системы[12].

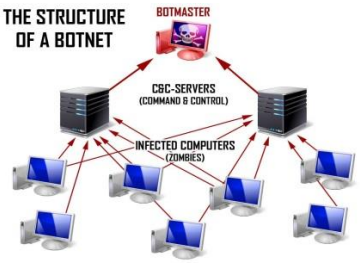
Использование или распространение вредоносных компьютерных программ и программных продуктов.



Потенциально нежелательные программы (ПНП или PUP) – могут являться разновидностью вредоносных программ. Их действие направлено на удаление необходимого программного обеспечения в компьютерной системе, установку приложений, шпионского или рекламного ПО. Каждый день в интернете появляются новые виды потенциально нежелательных программ.

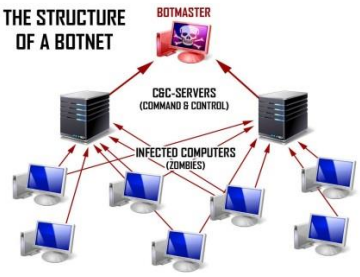
[12] https://ru.m.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82

Использование или распространение вредоносных компьютерных программ и программных продуктов.



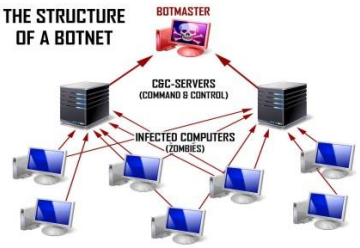
Backdoor (Бэкдор) – данный вид вредоносной программы предоставляет злоумышленнику возможность удаленно управлять зараженным компьютером. Такая программа способна выполнять на компьютере вообще любые действия, которые прикажет сделать ей создатель.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



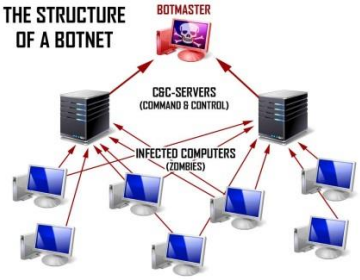
Downloader (Даунлоадер) – вредоносное программное обеспечение, позволяющее скачивать из интернета другие различные вирусы (трояны).

Использование или распространение вредоносных компьютерных программ и программных продуктов.



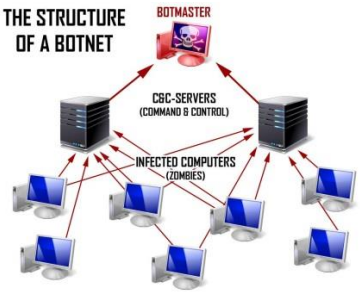
Dropper (Дроппер или Бомбосбрасыватель) – вредоносное программное обеспечение (вирус), предназначенное для установки на компьютер других вредоносных программ, которые могут содержаться в коде самого дроппера.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



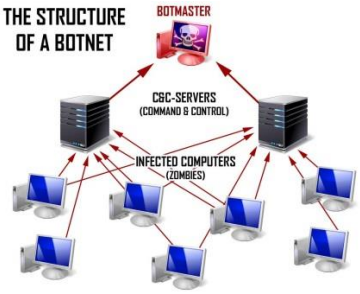
Exploit (Эксплойт) – это большое семейство вирусов, основная задача которых поиск уязвимостей в системе или отдельной программе с целью использования этой уязвимости для решения задач злоумышленника. Большинство взломов компьютерных серверов и сетей начинаются именно с попыток обнаружения или создания "дыр" в системе, для чего и используются эксплоиты.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



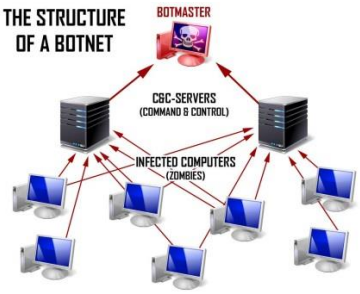
Hacking Tool (Хактул) – это вредоносная или потенциальная нежелательная программа для взлома определенных приложений. Представляет собой программный набор инструментов для подмены части кода или выполнения других действия над атакуемой программой. Яркий пример HackTool — любой кряк к платным играм и программным продуктам, делающий их «бесплатными».

Использование или распространение вредоносных компьютерных программ и программных продуктов.



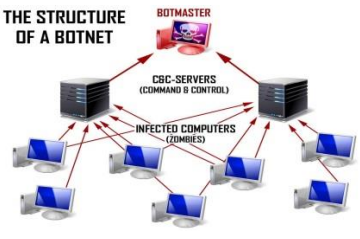
Macro virus (Макро-вирусы) – это вредоносный код, который выполняется в программах, поддерживающих написание пользовательский макросов (например, Microsoft Word или Excel). Макро-вирусы могут не только уничтожать/редактировать/пересылать документы, но и выполнять различные действия над другими файлами.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



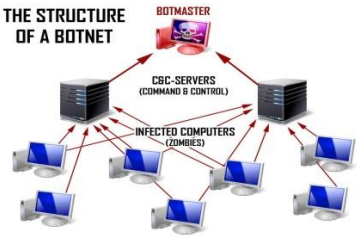
Obfuscator (Обфускатор) – программы для спутывания или подмены данных (как правило, исходных кодов других программ). Они могут использоваться для редактирования исходных кодов своих вирусов с целью усложнения их обнаружения антивирусами, а также для «обмана» приложений с целью открытия и запуска ими файлов, изначально не предназначенных для обработки в этом приложении.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



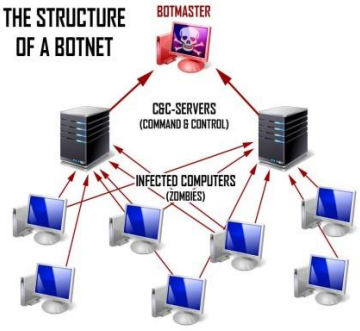
Password stealer (Похитители паролей) – программы, предназначенные для похищения пользовательских паролей из веб-форм или приложений, куда вводятся пароли. Зачастую такие вирусы идут «в комплекте» или являются частью кейлоггеров.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



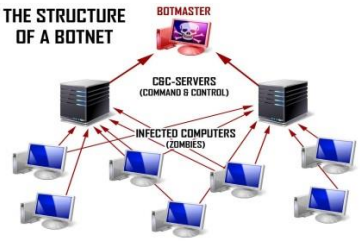
Keylogger (Кейлоггер) – шпионская программа, предназначенная для отслеживания нажатия клавиш, передвижение и клики мышью или вообще любые действия пользователя за компьютером с последующей отправкой собранной информации на компьютер злоумышленника.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



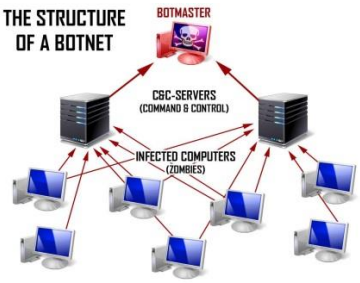
Ransomware (Вирус-вымогатель) – программа, предназначенная для выполнения каких-либо вредоносных действий с компьютером и/или данными с целью заставить владельца выплатить выкуп или совершить какое-либо действие. Она блокируют компьютер, шифруют важные файлы (фотографии, видео, документы и т.д.) или вовсе удаляют их без возможности восстановления, заранее отправляя злоумышленнику копии.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



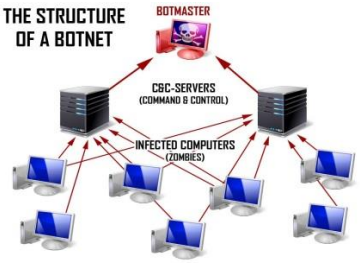
Rogue security software (Псевдоантивирусы**)** – программы, представляющиеся пользователю интернета как антивирусы, но на самом деле не являющиеся таковыми. Главная их задача заставить пользователя приобрести платную версию «антивируса».

Использование или распространение вредоносных компьютерных программ и программных продуктов.



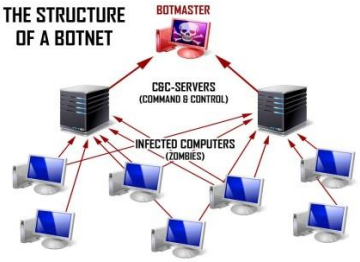
Trojan (Троян) – один из самых распространенных видов вирусных программ. Они обычно представляются обычными программами, могут даже быть полезными для пользователя до определенного момента. Пользователь устанавливает такую программу и даже работает с ней, а она параллельно выполняет указания злоумышленника.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



Trojan clicker (Троянский кликер) – вид трояна, обычно заражающих интернет-браузер (зачастую при установке расширений для браузера). Ее задача - переход по ссылкам, открытие в браузере рекламных сайтов и выполнения других действий в интернете.

Использование или распространение вредоносных компьютерных программ и программных продуктов.



Worm (Червь) – семейство вредоносных программ, предназначенных для повреждения данных на компьютере. Черви могут распространяться на другие компьютеры очень быстро, самыми различными путями — по почте, в сообщениях в мессенджерах, чатах и социальных сетях, в файлах и т.д.

Вопросы для самоконтроля:

1) Дайте характеристику уголовным правонарушениям, связанным с созданием и использованием вредоносных программ.

2) Что будет являться объектом данных уголовных правонарушений?

3) Дайте определение абонентскому устройству.

4) Что такое идентификационный код?

5) Назовите виды вредоносных программ применяемых при совершении киберпреступлений.

6) Для чего используются ботнеты?

IV группа: Хищения с использованием информационно-коммуникационных технологий (ИКТ**).**

Данная категория уголовных правонарушений охватывает такие составы преступлений как «*Кража, совершенная путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций» и «Мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы».*

Указанные виды преступлений являются наиболее распространенными и актуальными не только на территории Казахстана, но и других стран. В связи с чем, имеется необходимость разработки отдельных методик расследования преступлений, связанных с интернет - мошенничеством и кражей, совершенных с использованием ИКТ.

Для совершения вышеуказанных правонарушений преступник использует такие инструменты как создание вредоносного ПО, фишинг, социальный инжиниринг и т.д.

Объектом данной категории уголовных правонарушений будет являться собственность.

Предметом является имущество.

Объективная сторона выражается в форме действия, направленного на хищение чужой собственности, совершенного путем:

- незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций;
- обмана или злоупотребления доверием пользователя информационной системы».

Субъективная сторона предполагает только умышленную форму вины. Виновное лицо должно осознавать, что своими действиями оно причиняет собственнику материальный вред и желает этого.

Субъектом будут являться лица, достигшие 14 лет.

Для совершения данных видов уголовных правонарушений, преступники применяют различные виды кибератак.

Фишинг – это разновидность интернет мошенничества, применяемого для получения конфиденциальных данных. Например, логина и пароля от интернет-банкинга, номера банковской карты и другой важной информации.

Фишинговые сайты разрабатываются так, чтобы они выглядели как настоящие. Обычно они функционируют недолго, около 5-10 дней, так как их быстро обнаруживают антифишинговые программы.

Иногда для эффективности фишинговой атаки используются методы социальной инженерии, суть которой заключается в убеждении человека

любым способом предоставить свои конфиденциальные, идентификационные данные.

Сущность данного преступления заключается в том, что преступник создает какой-нибудь поддельный интернет ресурс (например, сайт банка или сайт крупного интернет магазина), с целью поймать доверчивого пользователя данных систем и похитить его деньги. Как только пользователь сети, находясь на поддельном сайте, попытается идентифицировать себя путем ввода логина и пароля, эти данные станут доступными интернет - мошеннику, который уже на настоящем сайте от имени вышеуказанного пользователя проникает в его интернет – банкинг и переводит деньги с его банковского счета на свой заранее открытый счет.

Побочным эффектом от этого преступления является получение преступником адреса электронной почты, которую он может использовать для совершения другого киберпреступления. Например, для совершения Ddos-атаки или регистрации на каком-нибудь интернет ресурсе.

Электронную почту также могут использовать для совершения преступления, связанного с проникновением в информационную систему (статья 205 УК РК).

Учитывая, что обналичивание похищенных денег оставляет множество электронных следов, «фишеры» в большинстве случаев, получив персональные данные пользователя сети, продают их другим киберпреступникам, в том числе через сеть даркнет.

Объектами фишинговых атак становятся банки, микрофинансовые организации, аукционы, различные электронные платежные системы, где есть возможность узнать и похитить идентификационные данные с целью завладения денежные средствами граждан.

Сложность расследования данного вида преступлений заключается в том, что оно не имеет границ.

Вопросы для самоконтроля:

1) Дайте характеристику уголовным правонарушениям, совершаемым с использованием информационно-коммуникационных технологий.

2) Что будет являться объектом данных уголовных правонарушений?

3) Дайте определение термину «фишинг».

4) Опишите принцип работы фишинговой атаки.

5)Назовите объекты фишинговых атак.

V группа: Уголовные правонарушения, связанные с незаконным контентом.

Указанная категория правонарушений включает в себя 2 состава: «*Неправомерное распространение электронных информационных ресурсов ограниченного доступа» и «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели».*

Несмотря на отсутствие зарегистрированных уголовных дел по данной категории, нельзя утверждать, что они не совершаются на территории Казахстана.

Все киберпреступления являются латентными, в связи с чем, процесс их выявления вызывает особые затруднения для следственно-оперативных подразделений правоохранительных органов.

Объектом данной категории уголовных правонарушений будут являться общественные отношения, связанные с обеспечением конфиденциальности персональных данных ограниченного доступа, связанные с обеспечением защищенности информационного пространства от материалов противоправного содержания.

К персональным данным относятся сведения об определенном субъекте, зафиксированные на электронном, бумажном и (или) ином материальном носителе, которые позволяют идентифицировать субъект. Они подразделяются на общедоступные и ограниченного доступа.

Предметом служат: электронные информационные ресурсы ограниченного доступа, сайты, преследующие противоправные цели.

Объективная сторона выражается в форме действия, направленного на неправомерное распространение электронных информационных ресурсов ограниченного доступа и предоставление услуг по предоставлению аппаратно-программных комплексов для размещения интернет-ресурсов, преследующих противоправные цели.

К интернет – ресурсам, преследующим противоправные цели, относятся материалы, содержащие пропаганду и оправдание экстремизма или терроризма, информацию, раскрывающую технические приемы и тактику антитеррористических операций в период их проведения, пропаганду наркотических средств, психотропных веществ и прекурсоров, культ жестокости, насилия, порнографии, а также вредоносные программы.

Субъективная сторона характеризуется только прямым умыслом.

Субъект специальный (собственник или владелец аппаратно-программных комплексов), лицо, достигшее 16 лет.

Деяние, предусмотренное частью 1 статьи 211 Уголовного кодекса Республики Казахстан, относится к уголовным проступкам.

Деяние, предусмотренное частью 2 статьи 211 Уголовного кодекса Республики Казахстан, относится к преступлениям средней тяжести.

Деяние, предусмотренное частью 3 статьи 211 Уголовного кодекса Республики Казахстан, относится к тяжким преступлениям.

Деяние, предусмотренное частью 1 статьи 212 Уголовного кодекса Республики Казахстан, относится к преступлениям небольшой тяжести.

Деяние, предусмотренное частью 2 статьи 212 Уголовного кодекса Республики Казахстан, относится к тяжким преступлениям.

Распространение незаконного или запрещенного контента

Распространение запрещенного / незаконного контента - преступление, представляющее собой распространение неприемлемого контента (неприятного и / или оскорбительного содержания). Например, видео с порнографией, насилием или любой другой преступной деятельностью. Незаконный контент включает материалы, связанные с экстремизмом, терроризмом, торговлей людьми, эксплуатацией детей и т.д.

Кибер-сталкинг - киберпреступление, включающее в себя онлайн-преследование. То есть, на пользователя обрушивается множество онлайн-сообщений и электронных писем неприятного содержания. Злоумышленники для совершения такого преступления используют социальные сети, веб-сайты, мессенджеры, поисковые системы. Главная их цель - запугать пользователя и внушить страх.

Кроме вышеуказанных уголовных правонарушений, к киберпреступлениям также можно отнести преступления, связанные с незаконным оборотом наркотических средств и оружия, торговлей людьми, терроризмом и экстремизмом, совершаемые посредством глобальной сети интернет и с помощью современных информационно-коммуникационных технологий (например, сотовых телефонов, мессенджеров и т.д.).

Вопросы для самоконтроля:

1) Дайте характеристику уголовным правонарушениям, связанным с незаконным контентом.

2) Что будет являться объектом данных уголовных правонарушений?

3) Дайте определение термину «кибер-сталкинг».

Международная кодировка киберпреступлений

Все коды, характеризующие компьютерные преступления имеют идентификатор, начинающийся с буквы Q. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного деяния.

Международная кодировка киберпреступлений представляет собой систему нумерации и описания киберпреступлений, которая позволяет установить единый язык обмена информацией между правоохранительными органами, юристами, экспертами и другими заинтересованными сторонами в различных странах.

Важными причинами использования вышеуказанной кодировки являются:

1. Единая классификация киберпреступлений (позволяет унифицировать классификацию киберпреступлений, чтобы облегчить сравнение и обмен информацией между разными странами, а также улучшает сотрудничество при расследовании киберпреступлений).

2. Улучшение сбора данных (ее использование позволяет стандартизировать сбор данных о киберпреступлениях и обмен информацией между странами, что существенно оказывает помочь в анализе глобальных тенденций в киберпреступности и разработке эффективных стратегий борьбы с ней).

3. Установление международного сотрудничества (она помогает различным странам работать вместе и сотрудничать в области предотвращения и расследования киберпреступлений, создает основу для обмена информацией о преступлениях и совместных операций между правоохранительными органами разных стран).

4. Нормативные и правовые цели (помогает развивать и улучшать законодательство, связанное с киберпреступностью, и устанавливать глобальные стандарты для борьбы с ней, что способствует укреплению правопорядка и защите интересов граждан в разных странах).

В целом, данная международная кодировка киберпреступлений необходима для понимания запроса иностранного правоохранительного органа, направленного в рамках оказания международной правовой помощи.

1	**QA**	**Несанкционированный доступ или перехват**	
2	*QAH*	*Компьютерный абордаж*	*Вид киберпреступления, связанного с незаконным проникновением в информационные сети.*
3	*QAI*	*Перехват*	*Вид киберпреступления, связанного с незаконным перехватом информации*

			через внешние коммуникационные системы или путем непосредственного подключения к линиям периферийных устройств. *Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе.*
4	*QAT*	*Кража времени*	*Вид киберпреступления, связанного с неоплатой услуг доступа в информационную систему или сеть электронно-вычислительной машины.*
5	*QAZ*	*Прочие виды несанкционированного доступа и перехвата*	
6	**QD**	**Изменение компьютерных данных**	
7	*QDL*	*Логическая бомба*	*Вид киберпреступления, связанного с внесением изменения в компьютерные данные без какого-либо разрешения собственника, путем внедрения логической бомбы или троянского коня.* *Логическая бомба – тайное встраивание в компьютерную программу вредоносной программы, которая срабатывает при наступлении определенных логических условий и после автоматически ликвидируется.*
8	*QDT*	*Троянский конь*	*Вид киберпреступления, связанного с тайным введением в чужое программное обеспечение вредоносной программы, позволяющей негласно осуществлять иные не планировавшиеся разработчиком программы функций.*

9	*QDV*	*Компьютерный вирус*	*Вредоносная программа для электронно-вычислительной машины, которая приводит к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы компьютера, системы или сети без предварительного предупреждения пользователя о характере действия программы и не запрашивающая его разрешения на реализацию программой своего назначения.*
10	*QDW*	*Компьютерный червь*	*Саморазмножающийся и само распространяющийся вирус, который специально создан для функционирования в сети ЭВМ.*
11	*QDZ*	*Прочие виды изменения данных*	
12	**QF**	**Компьютерное мошенничество (computer fraud)**	
13	*QFC*	*Мошенничество с банкоматами*	*Вид киберпреступления, связанного с хищением наличных денег из банкоматов.*
14	*QFF*	*Компьютерная подделка*	*Вид киберпреступления, связанного с хищением из компьютерных систем данных путем создания поддельных устройств (например, пластиковых карт).*
15	*QFG*	*Мошенничество с игровыми автоматами*	*Вид киберпреступления, связанного с игровыми автоматами.*
16	*QFM*	*Манипуляции с программами ввода вывода*	*Вид киберпреступления, связанного с программами ввода / вывода.*
17	*QFP*	*Мошенничества с платежными*	*Вид киберпреступления, связанного с хищением наличных денег (например, с*

		средствами	*пластиковых карт).*
18	*QFT*	*Телефонное мошенничество*	*Вид киберпреступления, связанного с незаконным доступом к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих системы электросвязи.*
19	*QFZ*	*Прочие компьютерные мошенничества*	
20	**QR**	**Незаконное копирование («пиратство»)**	
21	*QRG*	*Компьютерные игры*	*Вид киберпреступления, связанного с незаконным копированием, распространением или опубликованием компьютерных игр и другого программного обеспечения, защищенного законом об авторском праве и смежных правах.*
22	*QRS*	*Прочее программное обеспечение*	
23	*QRT*	*Топография полупроводниковых изделий*	*Вид киберпреступления, связанного с незаконным копированием топологии полупроводниковых изделий: копирование, без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.*
24	*QRZ*	*Прочее незаконное копирование*	
25	**QS**	**Компьютерный саботаж**	

26	*QSH*	*С аппаратным обеспечением*	*Вид киберпреступления, связанного с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.*
27	*QSS*	*С программным обеспечением*	*Вид киберпреступления, связанного с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.*
28	*QSZ*	*Прочие виды саботажа*	
29	**QZ**	Прочие компьютерные преступления	
30	*QZB*	*С использованием компьютерных досок объявлений*	*Вид киберпреступления, связанного с использованием электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности.*
31	*QZE*	*Хищение информации, составляющей коммерческую тайну*	*Вид киберпреступления, связанного с хищением информации, составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества.*
32	*QZS*	*Передача информации*	*Вид киберпреступления, связанного с использование компьютерных систем*

		конфиденциального характера	*или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характер.*
33	*QZZ*	*Прочие компьютерные преступления*	

Вопросы для самоконтроля:

1) Что представляет собой международная кодировка киберпреступлений?

2) Назовите причины использования данной международной кодировки?

3) Для чего нужна единая классификация киберпреступлений?

4. Технологии, используемые киберпреступниками

В современном информационном обществе сфера киберпреступности становится все более распространенной и опасной. Это вызывает необходимость изучения данного вопроса для лучшего понимания мотиваций и целей совершаемых преступлений, а также разработки эффективных стратегий предотвращения и борьбы с ними.

Для совершения уголовных правонарушений, в том числе в киберпространстве преступники используют все достижения современной науки и техники, передовые технологии и программное обеспечение, разрабатываемое или получаемое из открытых источников.

Вот несколько примеров того, какие технологии, вещи и предметы используют киберпреступники для совершения своих преступлений.

1. Мощные по техническим характеристикам компьютеры, ноутбуки и другие устройства, имеющие доступ к интернету. Они используются для взлома, распространения вредоносных программ, кражи данных и других видов атак.

2. Мобильные устройства. Современные смартфоны и планшеты также востребованы киберпреступниками. Они используются для отправки спама, фишинга, шпионажа и других видов атак на мобильные приложения и сети.

3. Устройства интернета вещей (IoT). Киберпреступники эксплуатируют уязвимости устройств IoT, таких как умные дома, видеонаблюдение, медицинские устройства и др., чтобы получить несанкционированный доступ, украсть данные или использовать их в качестве платформы для кибератак.

4. Специализированные устройства. К ним относятся инструменты, разработанные киберпреступниками, такие как скиммеры для кражи информации с банковских карт, аппаратные ключ логгеры, шифровальщики информации и другие специализированные устройства, предназначенные для выполнения конкретных видов атак.

5. Вредоносные программы и программное обеспечение. Киберпреступники используют широкий спектр вредоносных программ, таких как вирусы, черви, троянские программы, шпионское и рекламное программное обеспечение (adware), чтобы захватывать контроль над компьютерами и получать доступ к чувствительным данным.

6. Анонимизирующие инструменты. Киберпреступники могут использовать инструменты, которые помогают скрыть их идентификацию и местонахождение, такие как виртуальные частные сети (VPN), прокси-серверы и анонимные браузеры. Это позволяет им обходить меры безопасности и анонимно совершать киберпреступления.

7. Социальная инженерия. Наиболее мощным "инструментом" киберпреступников является способность манипулировать людьми. Они могут использовать фишинговые электронные письма, обманные звонки и

другие методы социальной инженерии, чтобы обмануть людей и получить доступ к их личной или корпоративной информации.

8. Компьютерные сети. Киберпреступники могут взламывать компьютерные сети, чтобы получить несанкционированный доступ к системам, украсть данные, внедрить вредоносные программы или нарушить работу сети. Они используют уязвимости в сетевых протоколах и системных службах для своих целей.

9. Ботнеты. Киберпреступники могут использовать ботнеты, которые представляют собой сети зараженных компьютеров, чтобы вести масштабированные атаки, отправлять спам, проводить DDoS-атаки (атаки отказом в обслуживании), распространять вредоносные программы и выполнить другие вредоносные операции. Компьютеры, зараженные зловредным программным обеспечением, становятся ботами, которыми киберпреступники могут удаленно управлять.

Это лишь некоторые примеры технологий, вещей и предметов, которые киберпреступники используют для совершения своих преступлений. Однако продолжающийся прогресс технологий и появление новых уязвимостей означает, что список этих инструментов будет продолжать расти.

5. Актуальные проблемные вопросы, связанные с выявлением и расследованием киберпреступлений

С каждым годом Казахстан, как и многие другие государства, отмечает рост киберпреступлений, которым становится всё сложнее противостоять.

Пока наши правоохранительные органы только начинают осваивать интернет пространство, преступные сообщества уже давно пошли вперед. Они научились скрывать следы своего пребывания в интернете, маскироваться, получать доступ ко всему, к чему у них есть интерес.

Рассмотрим и разберем основные проблемы, с которыми сталкиваются следственно-оперативные подразделения при выявлении и расследовании киберпреступлений.

Отсутствие специализированного подразделения по таким преступлениям во всех силовых ведомствах.

Пока не будет специализированных подразделений и лиц, непосредственно занимающихся исключительно только данным вопросом, работа в данном направлении будет идти тяжело.

Отсутствие специалистов по расследованию киберпреступлений в правоохранительных органах.

В большинстве своем проблема выявления и раскрытия данных преступлений связана с высокой профессиональной подготовкой преступника и сложной, с технической точки зрения, способом их совершения.

Поэтому их раскрытие зависит от профессиональных знаний сотрудника, занимающегося расследованием таких дел и умелым применением их на практике.

Отсутствие методических рекомендаций и алгоритмов расследования по всем видам киберпреступлений во всех силовых ведомствах.

Отсутствие или недостаточное количество методических рекомендаций, а также алгоритмов расследования по киберпреступлениям приводит к приостановлению процесса поиска преступника и утере электронных доказательств из-за неправильного обращения или не знания.

Недостаточное количество судебных экспертов по делам о киберпреступлениях.

Учитывая постоянный рост киберпреступлений, необходимо увеличить количество судебных экспертов, имеющих знания в сфере информационных технологий для проведения судебно-компьютерных экспертиз.

На сегодняшний день не в каждом регионе страны имеются такие специалисты в органах судебной экспертизы, что отражается на сроках расследования преступлений данной категории.

Отсутствие подготовленных судей и адвокатов по делам о киберпреступлениях.

Рассмотрение уголовных дел по киберпреступлениям в судах вызывает много вопросов со стороны, как адвокатов, так и судей, сталкивающихся со специфическими терминами и электронными доказательствами, значительно отличающихся от обычных своими свойствами. Для понимания процесса изъятия электронных доказательств и соотношения действий следователя или криминалиста с нормами уголовно-процессуального законодательства, требуется прохождение специальных учебных курсов.

Отсутствие специализированного программного обеспечения и соответствующего оборудования.

Отсутствие в правоохранительных органах специализированных программ и оборудования сильно ограничивает их возможности в анализе данных, поиске и изъятии цифровых доказательств.

Предложения по повышению эффективности выявления и расследования киберпреступлений

Для повышения эффективности выявления и расследования киберпреступлений предлагаются следующие меры:

1. Создание специализированных подразделений (управлений, отделов) во всех правоохранительных органах. Они будут заниматься исключительно выявлением и расследованием киберпреступлений. Это позволит сосредоточить ресурсы для более эффективного и оперативного реагирования на случаи совершения киберпреступления;
2. Установление международного сотрудничества между силовыми ведомствами различных стран с целью обмена информацией, методами и технологиями, связанными с выявлением и расследованием преступлений данной категории. Это позволит более эффективно пресекать деятельность киберпреступников, которые могут действовать за пределами одной страны;
3. Постоянное повышение уровня квалификации сотрудников правоохранительных органов. Это поможет значительно повысить уровень расследования и понимания новейших методов и тактик киберпреступников;
4. Использование технических и аналитических инструментов. Внедрение передовых технических и аналитических инструментов для обнаружения и анализа инцидентов киберпреступности. Машинное

обучение, искусственный интеллект и аналитические алгоритмы могут помочь обрабатывать большие объемы данных и выявлять скрытые связи и паттерны в поведении киберпреступников;

5. Установление более тесного взаимодействия и обмена информацией между правоохранительными органами и представителями гражданского общества, включая крупные компании, финансовые учреждения и другие организации. Это поможет быстрее и точнее выявлять и пресекать действия киберпреступников;

6. Совершенствование законодательства. Необходимость разработки и внедрения современного законодательства, направленного на пресечение и наказание киберпреступников;

7. Разработка и применение активных методов обнаружения киберпреступлений в режиме реального времени. То есть использование систем мониторинга, анализа событий и алгоритмов обнаружения аномалий для выявления подозрительной активности и атак на ранних стадиях.

Реализация данных предложений способствовала бы повышению эффективности и оперативности выявления и расследования киберпреступлений.

Комбинирование этих подходов позволит более эффективно бороться с быстро развивающейся киберугрозой.

Заключение

Угроза роста киберпреступности в мире по-прежнему сохраняется.

Несмотря на предпринимаемые властями разных стран предупредительные меры, направленные на защиту и обеспечение безопасности информационных систем государственных органов и граждан, правоохранительные органы регистрируют все новые и новые преступления в этой сфере.

Наряду с этим, происходит и рост количества киберпреступников, меняется их возрастной состав. Если раньше киберпреступником выступал в основном мужчина уже за 30 лет, то сейчас такие преступления совершают уже и молодые люди до 18 лет. Первым, что их вовлекает в среду киберпреступников, является «легкость заработка», а также «безнаказанность». Второе – это возможность заявить о себе, прославиться среди друзей, однокурсников и т.д.

Из-за анонимности и безнаказанности молодые хакеры совершают более серьезные преступления, которые потом выставляют напоказ перед знакомыми, друзьями с целью завоевания авторитета.

Самостоятельно решить эту проблему не способно ни одно государство мира. Поскольку данный вид преступлений не имеет границ и требует консолидаций усилий каждой страны, заинтересованной в борьбе с киберпреступностью.

В ходе данной работы автором были сформулированы понятия киберпреступности и киберпреступления, охарактеризованы виды киберпреступлений, рассмотрены способы их совершения.

Разработанное учебное пособие является основой знаний о киберпреступности и предназначено не только для использования в работе правоохранительных органов в расследовании киберпреступлений, но и для преподавателей, магистрантов и докторантов ВУЗов, в том числе специализированных.

Список использованных источников

1. Интернет-портал «Techopedia» [Электронный ресурс] – Режим доступа URL: https://www.techopedia.com/definition/4050/phreaking (дата обращения 08.06.2023).
2. Интернет-портал «TASS.RU» [Электронный ресурс] – Режим доступа URL: https://tass.ru/info/1408961 (дата обращения 08.06.2023).
3. Российская Ассоциация Электронных Коммуникаций. «Глобальные киберугрозы: возможно ли безопасное развитие цифровой инфраструктуры?»// [Электронный ресурс] – Режим доступа URL: http://raec.ru/live/raec-news/9471/ (дата обращения 08.06.2023).
4. Филимонов, В.П. Киберпреступность уже зашкаливает!/ В.П.Филимонов // Русская народная линия, информационно-аналитическая служба//[Электронный ресурс] - Режим доступа URL: http://ruskline.ru/special_opinion/2017/fevral/kiberprestupnost_uzhe _zashkalivaet/ (дата обращения 08.06.2023).
5. Интернет-портал «WebCanape» [Электронный ресурс] – Режим доступа URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/#:~:text=%D0%9F%D0%BE%20%D0%BF%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BD%D0%B8%D0%BC%20%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%BC%20ITU%20%D0%B8,%D0%BB%D0%B8%D1%88%D1%8C%20%D0%BD%D0%B0%2098%20%D0%BC%D0%B8%D0%BB%D0%BB%D0%B8%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%BF%D0%BE%D0% (дата обращения 15.06.2023).
6. Интернет-портал «Bizhit.ru» [Электронный ресурс] – Режим доступа URL: http://www.bizhit.ru/index/polzovateliinternetavmire/0-404 (дата обращения 18.06.2023).
7. Интернет-портал «Центр предпринимательских рисков» [Электронный ресурс] – Режим доступа URL: http://www.cprspb.ru/bibl/forein/21.htm (дата обращения 18.06.2023).
8. Департамент юстиции Акмолинской области [Электронный ресурс] – Режим доступа URL: https://www.gov.kz/memleket/entities/adilet-akm/press/article/details/103746?lang=ru (дата обращения 18.06.2023).
9. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК.
10. Интернет-портал «TengriNewsKz» [Электронный ресурс] – Режим доступа URL: https://tengrinews.kz/kazakhstan_news/otrajeno-20-millionov-atak-na-kaznet-gts-479742/ (дата обращения 20.06.2023).
11. Закон Республики Казахстан «О связи» от 5 июля 2004 года № 567.
12. Интернет сайт «Википедия» [Электронный ресурс] – Режим доступаURL:https://ru.m.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD% D0%B5 %D1%82 (дата обращения 20.06.2023).

Список дополнительной литературы

1. Шелупанов А.А., Смолина А.Р. Форензика. Теория и практика расследования киберпреступлений.-М.: Горячая линия - Телеком, 2020.-104 с.
2. Костин П.В., Комраков Н.Л. К вопросу о понятии исправности и работоспособности средств компьютерной техники // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).
3. Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации. // Конфидент. - С-Петербург, 1999, №4-5.
4. Расследование компьютерных преступлений. Вечерский Д.А Шалькевич И.И., Минск 2001с. 13с.
5. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: Дис.. канд. юрид. наук М.,1997. С. 83-101.
6. Родионов А. Н., Кузнецов А.В. Расследование преступлений в области высоких технологий // Вестник МВД России. 1999. № 6. С. 65-70.
7. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. М., 2001. С. 19-20.
8. Федоров В. Компьютерные преступления: выявление, расследование и профилактика // Законность, 1994. №6. С.44-47.
9. В.Б. Вехов. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: Учеб.-метод. Пос. Изд. 2-е, доп. И испр. – М.: МЦ при ГУК и КП МВД России, 2000. – 64 с.
10. Черных Э., Черных А. «Компьютерные» хищения: как их предотвратить? // Юстиция. 1993. №3. С. 21.
11. Крылов В.В. Расследование преступлений в сфере компьютерной информации. Криминалистика / Под ред. Н.П. Яблокова М., 1999. С. 620.
12. Головин А.Ю., Коновалов С.И., Толстухина Т.В. Тактика осмотра и обыска по делам о преступлениях в сфере компьютерной информации: Лекция. Тула, 2002.
13. Назмышев Р. А. Особенности и методические проблемы расследования неправомерного доступа к компьютерной информации. — Костанай, 2000. С. 15.
14. Касаткин А.В. Тактика собираний и использования компьютерной ин-формации при расследовании преступлений: Дис…. канд. юрид. Наук. М.,1997. С. 91.
15. Осипенко М. Компьютеры и преступность // Информационный бюллетень НЦБ Интерпола в Российской Федерации. 1994. № 10. С. 16.
16. Айков, Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: пер. с английского / Д. Айков, К. Сейгер, У. Фонсторх. – Москва: Мир, 1999. – 351 с.

17. Актуальные проблемы информационного права: учебник / Под ред. И. Л. Бачило, М. А. Лапина. – Москва: Юстиция, 2016. – 532 с.

18. Алексеев А.И. Криминологическая профилактика: теория, опыт, проблемы / А.И. Алексеев, С.И. Герасимов, А.Я. Сухарев. – Москва: Норма, 2001. – 496 с.

19. Анин Б.Ю. Защита компьютерной информации / Б. Ю. Анин. – Санкт-Петербург: БХВ - Санкт-Петербург, 2000. – 152 с.

20. Антонян Ю.М. Психология преступника и расследование преступлений / Ю. М. Антонян. – Москва: Юрист, 1996. – 335 с.

Приложение 1

Глоссарий

1. Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, зафиксированных в любой форме.

2. Целостность информации – это способность информации не изменяться, сохраняя первоначальное состояние.

3. Доступность информации – способность информационной системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями.

4. Компьютерная атака – целенаправленное и несанкционированное воздействие на информацию, электронный ресурс, информационную систему или получения доступа к ним с применением программных или программно-аппаратных средств.

5. Информационная система – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач.

6. Информационно-коммуникационные технологии – совокупность методов работы с электронными информационными ресурсами и методов информационного взаимодействия, осуществляемых с применением аппаратно-программного комплекса и сети телекоммуникаций.

7. Аппаратно-программный комплекс – совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа.

8. Программное обеспечение – совокупность программ, программных кодов, а также программных продуктов с технической документацией, необходимой для их эксплуатации.

9. Программный продукт – самостоятельная программа или часть программного обеспечения, являющаяся товаром, которая независимо от ее разработчиков может использоваться в предусмотренных целях в соответствии с системными требованиями, установленными технической документацией.

10. Блокчейн – информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования.

11. Аналитика данных – процесс обработки данных с целью получения информации и выводов для принятия решения.

12. Доменное имя – символьное (буквенно-цифровое) обозначение, сформированное в соответствии с правилами адресации Интернета, соответствующее определенному сетевому адресу и предназначенное для поименованного обращения к объекту Интернета.

13. Локальная сеть – часть сети телекоммуникаций, имеющая замкнутую инфраструктуру до точки подключения к другим сетям телекоммуникаций и обеспечивающая передачу информации и организацию совместного доступа к сетевым устройствам в территориально ограниченном пространстве объекта (помещение, здание, сооружение и его комплекс).

14. Интернет – всемирная система объединенных сетей телекоммуникаций и вычислительных ресурсов для передачи электронных информационных ресурсов.

15. Единый шлюз доступа к Интернету – аппаратно-программный комплекс, предназначенный для защиты объектов информатизации при доступе к Интернету и (или) сетям связи, имеющим выход в Интернет.

16. Интернет-ресурс – информация (в текстовом, графическом, аудиовизуальном или ином виде), размещенная на аппаратно-программном комплексе, имеющем уникальный сетевой адрес и (или) доменное имя и функционирующем в Интернете.

17. Абонент – физическое или юридическое лицо, с которым заключен договор на оказание услуг связи.

18. Абонентская линия - линия связи, являющаяся частью местной сети телекоммуникаций и соединяющая абонентское устройство со средствами телекоммуникаций этой сети.

19. Абонентское устройство - средство связи индивидуального использования, формирующее сигналы электрической связи для передачи или приема заданной абонентом информации и подключаемое к сети оператора связи.

20. Биллинг - аппаратно-программный комплекс, предназначенный для автоматического выполнения операций учета услуг, предоставляемых абонентам, а также их тарификации и выставления счетов для оплаты.

21. Сетевой трафик (далее – трафик) – объем информации, передаваемой и принимаемой через сеть телекоммуникаций за определенный период времени.

22. Интернет-трафик – объем информации, передаваемой и принимаемой через соединение с Интернетом за определенный период времени.

23. Владелец сети телекоммуникаций - физическое или юридическое лицо, которому принадлежит часть сети телекоммуникаций общего пользования и (или) соответствующая категория единой сети телекоммуникаций.

24. Сеть телекоммуникаций – совокупность средств телекоммуникаций и линий связи, обеспечивающих передачу сообщений телекоммуникаций, состоящая из коммутационного оборудования (станций, подстанций, концентраторов), линейно-кабельных сооружений (абонентских линий, соединительных линий и каналов связи), систем передачи и абонентских устройств.

25. Сотовая связь – вид электрической связи, использующей деление обслуживаемой территории на ряд ячеек, обеспечивающей возможность непрерывности связи при перемещении абонента из ячейки в ячейку и предназначенной для двустороннего (многостороннего) обмена информацией, передаваемой посредством радиоволн.

26. Оператор сотовой связи - оператор связи, предоставляющий услуги сотовой связи в соответствии с законодательством Республики Казахстан.

27. Пользователь информации – физическое или юридическое лицо, запрашивающее и (или) использующее информацию.

28. Хищение цифровой личности – это вид преступления, представляющий собой незаконное завладение учетной записью пользователя сети интернет для совершения мошенничества.

29. Учетная запись – совокупность сведений о пользователе, необходимая для его идентификации и предоставления доступа к личным данным и системным настройкам.

30. DoS и DDoS атаки – это вид кибератаки, целью которых является нарушение работы сайта или сервера (например, заполнения сервера пакетами TCP и UDP).

31. Ботнеты – это компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами, которые устанавливаются скрытно на устройство жертвы и позволяют злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера.

32. Потенциально нежелательные программы (ПНП или PUP) – разновидность вредоносных программ, действие которых направлено на удаление необходимого программного обеспечения в компьютерной системе, установку приложений, шпионского или рекламного ПО.

33. Backdoor (Бэкдор) – вид вредоносной программы, предоставляющий злоумышленнику возможность удалено управлять зараженным компьютером.

34. Downloader (Даунлоадер) – вредоносное программное обеспечение, позволяющее скачивать из интернета другие различные вирусы (трояны).

35. Dropper (Дроппер или Бомбосбрасыватель) – вредоносное программное обеспечение (вирус), предназначенное для установки на компьютер других вредоносных программ, которые могут содержаться в коде самого дроппера.

36. Exploit (Эксплойт) – это большое семейство вирусов, основная задача которых поиск уязвимостей в системе или отдельной программе с целью использования этой уязвимости для решения задач злоумышленника.

37. Hacking Tool (Хактул) – это вредоносная или потенциальная нежелательная программа для взлома определенных приложений.

38. Macro virus (Макро-вирусы) – это вредоносный код, который выполняется в программах, поддерживающих написание пользовательский макросов (например, Microsoft Word или Excel).

39. Obfuscator (Обфускатор) – программы для спутывания или подмены данных (как правило, исходных кодов других программ).

40. Password stealer (Похитители паролей) – программы, предназначенные для похищения пользовательских паролей из веб-форм или приложений, куда вводятся пароли.

41. Keylogger (Кейлоггер) – шпионская программа, предназначенная для отслеживания нажатия клавиш, передвижение и клики мышью или вообще любые действия пользователя за компьютером с последующей отправкой собранной информации на компьютер злоумышленника.

42. Ransomware (Вирус-вымогатель) – программа, предназначенная для выполнения каких-либо вредоносных действий с компьютером и/или данными с целью заставить владельца выплатить выкуп или совершить какое-либо действие.

43. Rogue security software (Псевдоантивирусы) – программы, представляющиеся пользователю интернета как антивирусы, но на самом деле не являющиеся таковыми.

44. Trojan (Троян) – один из самых распространенных видов вирусных программ. Они обычно представляются обычными программами, могут даже быть полезными для пользователя до определенного момента.

45. Worm (Червь) – семейство вредоносных программ, предназначенных для повреждения данных на компьютере.

46. Фишинг – это разновидность интернет мошенничества, применяемого для получения конфиденциальных данных.

47. Запрещенный / незаконный контент - преступление, представляющее собой распространение неприемлемого контента (неприятного и / или оскорбительного содержания).

48. Кибер-сталкинг - киберпреступление, включающее в себя онлайн-преследование.

49. Киберпреступление – это действия пользователя компьютерной системы, мобильной сети (сотовой связи), в том числе посредством сети интернет, против компьютерной системы, сети и данных, а также с помощью компьютерной системы, сети и данных.

50. Киберпреступник – это человек, который использует свои знания и современные технологии для совершения уголовных правонарушений с целью получения материальной выгоды или без таковой.

51. Хакер – специалист в области компьютерных систем и программ.

52. Фрикеры (Phreacker) – злоумышленники, специализирующиеся на совершении преступлений в области электросвязи, с использованием конфиденциальной компьютерной информации и специальных технических средств, разработанных (приспособленных, запрограммированных) для негласного получения (модификации, блокирования) информации с технических каналов электросвязи.

53. Крекеры (Cracker) – злоумышленники, осуществляющие «взлом» (модификацию, блокирование, уничтожение) средств защиты компьютерной информации.

54. Вирусописатели – злоумышленники, имеющие соответствующее образование или знания по созданию вредоносного программного обеспечения, для использования в совершении преступлений или без такового.

55. Кардеры (Carder) – злоумышленники, специализирующиеся на незаконной деятельности в сфере оборота пластиковых карт.

56. Скамеры (Scamer) – злоумышленники, которые занимаются получением, сбором личных сведений о пользователях сети интернет, с целью их использования в корыстных целях (например, получение денежных средств, подарков и т.д.).

57. Спамеры (Spamer) – злоумышленники, которые занимаются массовой рассылкой по электронной почте корреспонденции лицам, нежелающим ее получать.

Приложение 2

Для самоконтроля и проверки полученных знаний по пройденным темам предлагается примерный перечень тестовых вопросов, каждый из которых состоит из 4-х ответов (необходимо выбрать только один пункт).

Данная форма контроля дает возможность обучающимся выявить пробелы в своих знаниях, а преподавателю скорректировать учебный процесс с учетом результатов тестирования.

ПРИМЕРНЫЕ ТЕСТОВЫЕ ВОПРОСЫ
по теме: «Киберпреступность в современном мире: Основные понятия и тенденции»

1) Киберпреступление – это

а) активные действия пользователя компьютерной системы, против компьютерной системы, сети и данных, а также с помощью компьютерной системы, сети и данных;

б) активные действия пользователя компьютерной сети, совершаемые в организации, посредством изменения учетных данных пользователя;

в) активные действия пользователя компьютерной сети, совершаемые в рамках компьютерной системы, с помощью компьютерных данных;

г) активные действия пользователя компьютерной сети, совершаемые в киберпространстве с помощью устройств ввода компьютерных данных.

2) Причины распространения киберпреступлений

а) увеличение количества времени пребывания пользователя информационной системы в сети интернет;

б) увеличение объема внутренней и внешней памяти устройства (компьютера, ноутбука, планшета и т.д.);

в) увеличение количество компьютерных данных в устройстве, информационной системе, интернете;

г) увеличение количества пользователей сети интернет.

3) Дайте определение хищению цифровой личности

а) вид преступления, представляющий собой незаконное завладение учетной записью пользователя сети интернет;

б) вид преступления, представляющий собой незаконное предоставление прав пользователю сети интернет;

в) вид преступления, представляющий собой отказ в предоставлении учетной записи пользователя сети интернет;

г) вид преступления, представляющий собой незаконное создание и использование учетной записи пользователя сети интернет.

4) Что является предметом уголовных правонарушений, связанных с незаконным контентом?

а) электронные информационные ресурсы;

б) информация и иные электронные данные;

в) внешняя и внутренняя память компьютера;

г) устройства ввода и вывода информации.

5) Какая форма мотивации киберпреступников описывает кибератаки, связанные с политическими акциями?

а) хактивизм;

б) вандализм;

в) месть;

г) материальная выгода.

6) Как называются злоумышленники, которые занимаются массовой рассылкой по электронной почте корреспонденции лицам, нежелающим ее получать?

а) скамеры;

б) спамеры;

в) кардеры;

г) крекеры.

7) Как называются злоумышленники, осуществляющие «взлом» (модификацию, блокирование, уничтожение) средств защиты компьютерной информации?

а) фрикеры;

б) крекеры;

в) вирусописатели;

г) кардеры.

8) Какие незаконные действия относятся к преступлениям против конфиденциальности, целостности и доступности компьютерных данных и систем?

а) незаконный перехват и воздействие на информационную систему;

б) мошенничество с использованием компьютерных технологий;

в) нарушение авторского права, смежных прав;

г) подлог с использованием компьютерных технологий.

9) Какие незаконные действия относятся к преступлениям, связанным с содержанием контента?

а) детская порнография;

б) незаконный доступ;

в) воздействие на данные (информацию);

г) незаконный перехват.

10) Что такое bot net (ботнет)?

а) большие сети из устройств пользователей, зараженных вредоносными программами;

б) один из разновидностей темного интернета, находящегося в свободном доступе;

в) наименование специализированной программы для подключения к глобальной сети интернет;

г) наименование программы для общения по закрытой информационной системе.

11) Что является предметом уголовного правонарушения «Неправомерное уничтожение или модификация информации»?

а) информация;

б) компьютер;

в) принтер;

г) системный файл;

12) Кто будут являться субъектом уголовного правонарушения «Неправомерное уничтожение или модификация информации»?

а) физическое вменяемое лицо, достигшее 16 лет;

б) физическое вменяемое лицо, достигшее 14 лет;

в) физическое вменяемое лицо, достигшее 18 лет;

г) физическое вменяемое лицо, достигшее 21 года.

Приложение 3

Решение ситуационных задач позволяет развить необходимые обучающимся навыки, такие как: проведение аналитической работы, планирование, поиск собственных подходов к решению нестандартных ситуаций, умение определять главные задачи и приоритетность их выполнения.

Выполнение заданий предполагает письменную форму ответа по каждому поставленному вопросу.

СИТУАЦИОННЫЕ ЗАДАЧИ
по теме: по теме: «Киберпреступность в современном мире: Основные понятия и тенденции»

Задача № 1

Тимуров А., используя свои знания в программировании, проник в социальной сети «В контакте» на личную страницу, принадлежащую Самариной О., и поменял пароли, в том числе от ее почтового ящика. В дальнейшем Тимуров А. стал переписываться от имени Самариной О. с мужчинами, выставляя фотографии порнографического содержания.

Вопросы:

1) Квалифицируйте действия Тимурова А.

2) С какого возраста наступает уголовная ответственность за совершение вышеуказанного уголовного правонарушения?

Задача № 2

Сабитов К. написал вредоносное программное обеспечение, которое вместе с письмом и файлом «Отчет-2023» направил по электронной почте в ТОО «Квартал». Данное письмо было открыто сотрудниками бухгалтерии, после чего Сабитов получил доступ к операционной системе бухгалтерских компьютеров. Имея функцию удаленного доступа, он в отсутствии сотрудников бухгалтерии перевел денежные средства в сумме 5 млн. тенге со счета ТОО «Квартал» на свой лицевой счет Каспи банка.

Вопросы:

1) Квалифицируйте действия Сабитова К.

2) Укажите объект и предмет уголовного правонарушения, совершенного Сабитовым К.

Задача № 3

Смагулов О. приобрел через интернет устройство по сканированию мобильных телефонов. С помощью данного устройства, он перехватил

несколько идентификационных кодов мобильных телефонов граждан, которые потом использовал для звонков на зарубежные номера.

В результате указанных действий 3 гражданам был причинен материальный ущерб на сумму более 250 тыс. тенге.

Вопросы:

1) *Подлежит ли Смагулов О. уголовной ответственности?*
2) *Квалифицируйте действия Смагулова О.*

Задача № 4

Иванов К., работая в частной клинике «Медсервис», незаконно проникнул в ее информационную базу, откуда скачал истории болезней 10 пациентов. Далее, используя информацию из истории болезней, он стал их шантажировать.

Вопросы:

1) *Подлежит ли Смагулов О. уголовной ответственности?*
2) *Квалифицируйте действия Смагулова О.*

Приложение 4

Примерный перечень вопросов к экзамену
по теме: «Киберпреступность в современном мире: основные понятия и тенденции»

1) История зарождения и развития киберпреступности.
2) Понятие и виды киберпреступлений.
3) Причины распространения киберпреступлений.
4) Методы и способы совершения киберпреступлений.
5) Киберпреступники и их разновидности.
6) Мотивация киберпреступников.
7) Проблемные вопросы, связанные с выявлением и расследованием киберпреступлений.
8) Технологии, используемые киберпреступниками.
9) Неправомерный доступ в информационную систему или сеть телекоммуникаций.
10) Нарушение работы информационной системы или сетей телекоммуникаций.
11) Неправомерный доступ к информации.
12) Неправомерное уничтожение или модификация информации.
13) Неправомерное завладение информацией.
14) Принуждение к передаче информации.
15) Создание, использование или распространение вредоносных компьютерных программ и программных продуктов.
16) Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства.
17) Кража, совершенная путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.
18) Мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы.
19) Неправомерное распространение электронных информационных ресурсов ограниченного доступа.
20) Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели.

Приложение 5

Примерная модель учебной программы

Обучающий курс на тему: «Киберпреступность в современном мире: основные понятия и тенденции»

Обоснование

С появлением Интернета и стремительным развитием новых технологий, традиционная преступность постепенно стала переходить в виртуальный мир.

Этому способствовали следующие факторы:

- *широкое распространение информационно-коммуникационных технологий;*
- *легкость и доступность всевозможных средств и методов для незаконного получения финансовых средств;*
- *скрытость и анонимность всех действий;*
- *отсутствие границ для совершения правонарушений;*
- *не готовность наших правоохранительных органов противостоять ее развитию и распространению.*

Ни для кого не секрет, что большинство таких преступлений остаются не раскрытыми. Следственно-оперативные подразделения правоохранительных органов испытывают недостаток кадровых специалистов, разбирающихся в IT-технологиях.

В связи с чем, имеется необходимость в подготовке сотрудников правоохранительных органов по направлению: «Расследование киберпреступлений».

Программа курса разработана с учетом минимальных требований к уровню их знаний для понимания процесса совершения компьютерных преступлений

Цель курса – повышение квалификации слушателей по вопросам расследования уголовных правонарушений, совершенных с использованием Интернета.

Задачи курса – ознакомить слушателей с видами и методами совершения киберпреступлений, лицами их совершающих, а также с мерами противодействия киберпреступности.

Продолжительность курса – 12 академических часов.

В ходе занятий акцентируется внимание слушателей на разделах, требующих самостоятельного освоения.

Изучение курса предусматривает входной и выходной *(рубежный)* контроль в виде тестирования. Может применяться промежуточный контроль

(по усмотрению преподавателя), который осуществляется в виде подготовки слушателями презентаций по выбранной теме *(в программе Ms. PowerPoint)*.

Для проведения курса требуется:

- аудитория, оборудованная компьютерной техникой и высокоскоростным интернетом *(стандартный настольный компьютер с операционной системой «Microsoft Windows» не ниже 10 версии)*.

Ожидаемый эффект

Подготовка квалифицированных специалистов для правоохранительных органов, готовых расследовать отдельные виды компьютерных преступлений.

Ниже представлена примерная программа курса для освоения темы: «Киберпреступность в современном мире: основные понятия и тенденции».

ПРОГРАММА КУРСА

№	Темы обучения	Описание тем	Часы
1	Введение в киберпреступность	Данная тема раскрывает понятие киберпреступности, тенденции в области развития Интернета и технологий, а также описывает проблемы технического, правового, этического и оперативного характера, связанные с расследованием киберпреступлений.	3ч
2	Классификация киберпреступлений, их основная характеристика, методы и способы совершения	Данная тема раскрывает основные категории и типы киберпреступлений.	7ч
3	Актуальные проблемные вопросы, связанные с выявлением и расследованием киберпреступлений	Данная тема раскрывает проблемные вопросы, связанные с выявлением и расследованием киберпреступлений	2ч
Итого:			**12ч**

Приложение 6

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Уголовный кодекс Республики Казахстан (выдержки из кодекса)

Глава 6. Уголовные правонарушения против собственности

Статья 188. Кража

2. Кража, совершенная:

4) путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций, – наказывается штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до одной тысячи двухсот часов, либо ограничением свободы на срок до пяти лет, либо лишением свободы на тот же срок, с конфискацией имущества.

Статья 190. Мошенничество

2. Мошенничество, совершенное:

4) путем обмана или злоупотребления доверием пользователя информационной системы - наказывается штрафом в размере до четырех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до одной тысячи часов, либо ограничением свободы на срок до четырех лет, либо лишением свободы на тот же срок, с конфискацией имущества, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 195. Причинение имущественного ущерба путем обмана или злоупотребления доверием

3. Причинение имущественного ущерба собственнику или иному владельцу имущества, совершенные:

3) путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций, – наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Глава 7. Уголовные правонарушения в сфере информатизации и связи

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

1. Умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказывается штрафом в размере до ста шестидесяти месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста шестидесяти часов, либо арестом на срок до сорока суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние, совершенное в отношении критически важных объектов информационно-коммуникационной инфраструктуры, – наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до двухсот часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, – наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 206. Неправомерные уничтожение или модификация информации

1. Умышленные неправомерные уничтожение или модификация охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, а равно ввод в информационную систему заведомо ложной информации, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказываются штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до

двухсот часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. Те же деяния, совершенные:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору, – наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций

1. Умышленные действия (бездействие), направленные на нарушение работы информационной системы или сетей телекоммуникаций, – наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. Те же деяния, совершенные:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору, – наказываются штрафом в размере до четырех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до одной тысячи часов, либо ограничением свободы на срок до четырех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, – наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Статья 208. Неправомерное завладение информацией

1. Умышленное неправомерное копирование или иное неправомерное завладение охраняемой законом информацией, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние, совершенное:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору, – наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 209. Принуждение к передаче информации

1. Принуждение к передаче охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, под угрозой применения насилия либо уничтожения или повреждения имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или

его близких, либо иных сведений, оглашение которых может причинить существенный вред интересам потерпевшего или его близких, – наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние:

1) сопряженное с применением физического насилия над лицом или его близкими;

2) совершенное группой лиц по предварительному сговору;

3) совершенное с целью получения информации из критически важных объектов информационно-коммуникационной инфраструктуры, – наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, – наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

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

1. Создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно умышленные использование и (или) распространение такой программы или программного продукта – наказываются штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до восьмисот часов, либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или

заниматься определенной деятельностью на срок до трех лет или без такового.

2. Те же деяния, совершенные:

1) группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения;

3) в отношении критически важных объектов информационно-коммуникационной инфраструктуры, – наказываются ограничением свободы на срок от трех до семи лет либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, – наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа

1. Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем, – наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, совершенное:

1) группой лиц по предварительному сговору;

2) из корыстных побуждений;

3) лицом с использованием своего служебного положения, – наказывается привлечением к общественным работам на срок до одной тысячи двухсот часов либо ограничением свободы на срок до пяти лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные

должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

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

1. Заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в открытой информационно-коммуникационной сети, для размещения интернет-ресурсов, преследующих противоправные цели, – наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или преступной группой, – наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

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

1. Изменение идентификационного кода абонентского устройства сотовой связи, создание дубликата карты идентификации абонента сотовой связи, если эти действия совершены без согласия производителя или законного владельца, – наказываются штрафом в размере до ста шестидесяти месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста шестидесяти часов, либо арестом на срок до сорока суток.

2. Неправомерные создание, использование, распространение программ, позволяющих изменять идентификационный код абонентского устройства сотовой связи или создавать дубликат карты идентификации абонента сотовой связи, – наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные преступной группой, – наказываются лишением свободы на срок до пяти лет.

Концепция кибербезопасности ("Киберщит Казахстана"),
утвержденная постановлением Правительства Республики Казахстан
от 30 июня 2017 года № 407.

Содержание

1. Введение

Концепция кибербезопасности ("Киберщит Казахстана") (далее – Концепция) разработана в соответствии с Посланием Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира.

Концепция основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития "цифровой" экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг.

Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий (далее – ИКТ).

Концепция призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

При разработке Концепции изучен международный опыт в области формирования подходов к защите национальной информационно-коммуникационной инфраструктуры государств-лидеров в сфере разработки и использования информационно-коммуникационных технологий, так и стран, стремящихся расширить сферу их применения для достижения целей социально-экономического развития.

Выполнение данной Концепции послужит дальнейшей модернизации казахстанского общества и станет вкладом Казахстана в реализацию Глобальной программы кибербезопасности ООН.

Термины и определения

Для целей настоящей Концепции под кибербезопасностью понимаются состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации.

Защита информации или электронных информационных ресурсов и информационных систем – комплекс физических, технических, программных, криптографических и административных мер, направленных на обеспечение информационной безопасности.

Классическая модель информационной безопасности базируется на обеспечении трех значимых для безопасности информации атрибутов: конфиденциальность, целостность и доступность.

Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.

Если доступ к информации получает неуполномоченное лицо, происходят несанкционированный доступ или нарушение конфиденциальности.

Для некоторых видов защищаемых законом или владельцем типов информации конфиденциальность является одним из наиболее важных атрибутов (служебная информация, охраняемые законом виды тайн, персональные данные ограниченного доступа, например, сведения о клиентах банка, кредиторах, налоговые данные, сведения медицинских учреждений о состоянии здоровья пациентов и т. д.).

Целостность информации – способность информации (данных) сохраняться в неискаженном виде. Неправомочные и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к нарушению целостности.

Особенно важна целостность данных, связанных с функционированием объектов критической информационно-коммуникационной инфраструктуры (например, автоматизированные системы управления воздушным движением, электро и энергоснабжения и так далее).

Доступность информации определяется способностью информационной системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Уничтожение или блокирование информации (в результате ошибки или преднамеренного действия) приводят к потере доступности.

Доступность – важный атрибут для функционирования информационных систем, ориентированных на обслуживание клиентов путем предоставления информационно-коммуникационных услуг (информационные системы продажи железнодорожных и авиационных билетов, банковских услуг, распространение продукции Интернет-ресурсами и электронными СМИ в Интернете). Ситуацию, когда уполномоченный пользователь не может получить доступ к определенным услугам (чаще всего сетевым), называют отказом в обслуживании.

В связи с развитием коммуникационных (сетевых технологий) также дополнительно выделяют еще два свойства информационной безопасности, связанные с личностью лица, управляющего или использующего информационную систему или электронный информационный ресурс с использованием сети удаленно: аутентичность и апеллируемость.

Аутентичность – возможность достоверно установить автора юридически значимого действия с информацией или сообщения в сфере оказания информационно-коммуникационных услуг, например, в электронной коммерции, когда используются электронно-цифровая подпись или иной способ аутентификации.

Апеллируемость (неотрекаемость) – возможность при отказе от авторства доказать, что автором действий с информацией в информационной системе или ресурсе является именно данный пользователь и никто другой путем регистрации совершаемых действий.

Аутентификация (установление подлинности) – проверка принадлежности к субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Идентификация – присвоение субъектам доступа к информационной системе или электронному ресурсу личного идентификатора, обеспечивающего установление подлинности и определение полномочий субъекта при его допуске в информационную систему, контроль полномочий в процессе сеанса работы и регистрацию действий.

Идентификация и аутентификация – основа современных программно-технических средств безопасности, так как любые ИКТ-услуги и сервисы в основном рассчитаны на обслуживание субъектов-пользователей.

Угроза информационной безопасности – потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или компоненты информационной системы или ресурса могут прямо или косвенно привести к нанесению ущерба интересам владельцев и пользователей.

Наиболее распространенные угрозы информационной безопасности – это сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и так далее), неправильное хранение архивных данных, нарушения прав доступа к данным, некорректная работа пользователей и обслуживающего персонала, потери информации (из-за

несанкционированного доступа или инфицирования вредоносными программами – компьютерными вирусами).

Компьютерная атака – целенаправленная попытка реализации угрозы несанкционированного воздействия на информацию, электронный ресурс, информационную систему или получения доступа к ним с применением программных или программно–аппаратных средств (или протоколов межсетевого взаимодействия).

Все иные термины приведены в значениях, используемых в Конституции Республики Казахстан, Уголовном кодексе Республики Казахстан, Кодексе Республики Казахстан "Об административных правонарушениях", законах Республики Казахстан "О национальной безопасности Республики Казахстан", "О государственных секретах", "О противодействии терроризму", "Об электронном документе и электронной цифровой подписи", "Об информатизации", "О техническом регулировании", "О разрешениях и уведомлениях", "О средствах массовой информации", "О связи", "О персональных данных и их защите", "О доступе к информации" и национальных технических стандартах.

2. Анализ текущей ситуации

Характерная для последних десятилетий общемировая тенденция внедрения достижений информационно-коммуникационных технологий с темпами, существенно опережающими формирование культуры их использования, и укоренения общественных и производственных отношений, характерных для "информационного общества", в первую очередь, в вопросах обеспечения кибербезопасности, в Казахстане также находит свое подтверждение.

Тем не менее, начиная с 1998 года, 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" (2003, 2007, 2015 годы) и несколько специализированных законов Республики Казахстан о внесении в них соответствующих изменений по вопросам электронных форматов представления информации (данных) в том числе по вопросам информационно-коммуникационных сетей, "электронного правительства".

За прошедший период электронные информационные ресурсы и информационные системы введены в хозяйственный оборот наряду с другими видами имущественных активов, расширена сфера их рыночного использования.

Сфера автоматизации государственных услуг, рынок электронной коммерции и электронных платежей развиваются на принципах обеспечения безопасности личности, общества и государства при применении информационно-коммуникационных технологий, а также осуществления

деятельности на основе единых стандартов, обеспечивающих надежность и управляемость объектов информатизации и связи.

С этапа становления вопросов информационной безопасности с учетом характера содержащейся информации дифференцированы правовые режимы общедоступных и конфиденциальных электронных информационных ресурсов и систем, установлены права и обязанности собственников, владельцев и пользователей по их защите.

Деятельность государственных органов и других субъектов по обеспечению информационной безопасности в области информатизации и связи осуществляется в соответствии с их отраслевой компетенцией, а также целями и задачами в предметных областях, связанных с использованием ИКТ (регулирование связи и информационных технологий, защита персональных данных, защита государственных секретов, противодействие деятельности иностранных технических разведок, оперативно-розыскная деятельность на сетях связи, расследование преступлений, совершаемых с использованием ИКТ и другие).

В целом, в Республике Казахстан организационно-правовые и технические основы системы мер по обеспечению информационной безопасности в области информатизации и связи (кибербезопасности) формировались и законодательно закреплялись как составляющие информационной безопасности и обеспечения безопасности информационного пространства и инфраструктуры связи в соответствии с Законом Республики Казахстан "О национальной безопасности".

В последние годы различные взаимоувязанные аспекты обеспечения информационной безопасности в области информатизации и связи нашли свое отражение и развитие в Уголовном кодексе Республики Казахстан, Кодексе Республики Казахстан "Об административных правонарушениях", законах Республики Казахстан "О государственных секретах", "О персональных данных и их защите", "Об электронном документе и электронной цифровой подписи", "О связи", и целом ряде подзаконных актов, разработанных в реализацию новой редакции Закона Республики Казахстан "Об информатизации", вступившего в силу с 1 января 2016 года.

Ряд подзаконных актов, принятых в последнее время, еще не получил развернутой правоприменительной практики. В частности, постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности" (далее – Единые требования), представляющих собой кодификацию правовых и технических норм из национальных и гармонизированных стандартов. Документ подробно описывает процедуры и правила по использованию информационно-коммуникационных технологий при обработке защищаемых законом видов информации, содержит важные нормы по обеспечению технологической безопасности информационной

инфраструктуры, информационных систем и ресурсов, программного обеспечения, технических средств на всех этапах их жизненного цикла.

На законодательном уровне регламентировано функционирование системы мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства", включающих в себя как государственные, так и негосударственные информационные системы, интегрируемые с государственными.

В Правилах проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства", утвержденных приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66, заложены основные принципы взаимодействия между заинтересованными сторонами при технологических сбоях или признаках компьютерных атак, а также алгоритмы реагирования на возникающие события и инциденты информационной безопасности.

Центр мониторинга безопасности "электронного правительства" ежедневно выявляет не устраненные уязвимости, о чем для принятия мер направляет уведомления владельцам информационных систем, являющиеся его компонентами. Имеется положительная динамика выявляемых уязвимостей и принимаемых в отношении них мер. Так в 2014 году было выявлена 1241 не устраненная уязвимость, в 2015 – 469, в 2016 – 355.

Также постановлением Правительства Республики Казахстан от 8 сентября 2016 года № 529 утверждены Правила и критерии отнесения объектов к критически важным объектам информационно-коммуникационной инфраструктуры из числа особо важных государственных и стратегических объектов, а также объектов отраслей экономики, имеющих стратегическое значение.

На подобные объекты, вошедшие в перечень критически важных объектов информационно-коммуникационной инфраструктуры, распространяются Единые требования, а также необходимость участия в предусмотренных законодательством совместных мероприятиях по обеспечению мониторинга их информационной безопасности, защиты и безопасного функционирования, включая обязанность информирования об инцидентах информационной безопасности.

Совершенствуются процедуры введения информационных систем в промышленную эксплуатацию. В этой связи, законодательно дифференцированы меры безопасности к информационным системам в зависимости от их отнесения к определенному классу, ограничен срок нахождения информационной системы в режиме опытной эксплуатации.

На соответствие требованиям информационной безопасности проведено более 500 аттестационных обследований государственных и негосударственных информационных систем, интегрируемых с государственными, по результатам которых выдано 199 аттестатов,

являющихся основанием для введения в промышленную эксплуатацию. Оставшаяся часть информационных систем в соответствии с Законом Республики Казахстан "Об информатизации" должны быть аттестована до конца 2018 года.

С 1 января 2016 года информационные системы государственных органов, негосударственные информационные системы, интегрируемые с государственными информационными системами на этапе опытной эксплуатации, проходят испытания на соответствие требованиям информационной безопасности. Во время испытаний проверке подвергаются исходные коды, настройки функций безопасности, обследуется сетевое и серверное оборудование и осуществляется нагрузочное тестирование.

Результаты проведения испытаний отражаются в повышении защищенности и отказоустойчивости информационных систем, безопасности программного обеспечения информационных систем, снижении влияния факторов нарушений информационной безопасности информационных систем, внедрении механизмов контроля и мониторинга безопасности информационных систем.

Система технического регулирования предусматривает подтверждение соответствия программного обеспечения и телекоммуникационного оборудования, в том числе с определением случаев их обязательной сертификации при использовании в государственном секторе. В этих целях ежегодно актуализируется свод национальных и гармонизированных технических стандартов в сфере информационной безопасности, защиты информации, безопасности информационных технологий. В настоящее время это 68 технических стандартов.

Благодаря централизации подключения к Интернету через Единый шлюз доступа к Интернету государственных органов существенно снижены угрозы несанкционированного доступа и вредоносного воздействия на электронные информационные ресурсы государственных органов. На ежедневной основе фиксируется и отражается более 180 миллионов атак различного уровня.

Создана и совершенствуется система правовых, организационных, технических и криптографических мер защиты государственных секретов, обрабатываемых с использованием средств вычислительной техники.

Наиболее чувствительная для безопасности государства информация в электронной форме передается только через сети телекоммуникаций специального назначения, физически отделенные от Интернета и использующие криптографические средства защиты информации.

Подходы к обеспечению безопасности инфраструктуры связи и сетей телекоммуникаций общего пользования выстраиваются вокруг системы централизованного управления сетями телекоммуникаций, через возможности магистральных операторов связи, реализующих на пограничном оборудовании концепцию "электронной границы".

Национальный сегмент Интернета насчитывает более 120 тысяч Интернет-ресурсов в доменах .KZ и .ҚАЗ, в соответствии с законодательством физически размещаемых на территории Республики Казахстан. В целях оказания содействия владельцам и пользователям информационных ресурсов и систем по вопросам безопасного использования ИКТ с 2010 года функционирует национальная Служба реагирования на компьютерные инциденты KZ-CERT. Служба является участником ряда международных организаций, в т.ч. FIRST (Forum of Incident Response and Security Teams), TI (Trusted Introducer for Security and Incident Response Teams), OIC-CERT (Организация исламского взаимодействия Служб реагирования на компьютерные инциденты).

Службой заключено 20 меморандумов о взаимопонимании и сотрудничестве с профильными структурами зарубежных стран, зафиксировано и обработано более 66 тысяч инцидентов информационной безопасности.

На казахстанском рынке появились первые отечественные компании, занимающиеся инструментальным аудитом по оценке защищенности (тестированием на проникновение) на соответствие требованиям информационной безопасности и специализирующиеся на исследовании обстоятельств, причин и условий инцидентов информационной безопасности, а также техническом исследовании вредоносного программного обеспечения. Разработаны первые отечественные средства антивирусной защиты.

В ряде национальных компаний и частных структурах существуют подразделения мониторинга технических событий и технологических процессов, которые в круглосуточном режиме ведут дежурство для оперативного реагирования на внештатные ситуации.

Законодательно определены цели сбора, обработки персональных данных граждан в электронном виде, а также порядок и меры по их защите. Законодательство регламентирует как процедуры их сбора исключительно с согласия граждан, так и уничтожения по их требованию операторами персональных данных, а также условия безопасного хранения персональных данных на территории страны и их трансграничной передачи.

Требования по безопасности банковских информационных систем обеспечиваются нормативно-правовыми актами Национального Банка Республики Казахстан с учетом отраслевых и международных требований по обеспечению безопасности информационных систем.

Новая редакция Уголовного кодекса Республики Казахстан, действующая с 2014 года, предусматривает отдельную главу, посвященную преступлениям, совершаемым в сфере информатизации и связи. С учетом квалифицирующих обстоятельств в ней содержится 38 составов преступлений против электронных информационных ресурсов и систем или сетей телекоммуникаций.

Кодекс Республики Казахстан "Об административных правонарушениях" также содержит ряд составов административных правонарушений, за совершение которых предусмотрены меры административной ответственности, в том числе на должностных лиц, не выполняющих обязанности по обеспечению информационной безопасности в виде нарушения требований по эксплуатации средств защиты электронных информационных ресурсов, невыполнения Единых требований, неосуществления или ненадлежащего осуществления собственником или владельцем информационных систем, содержащих персональные данные, мер по их защите.

На сегодняшний день в учебные планы специальности "Системы информационной безопасности" кроме изучения прикладных дисциплин включены дисциплины, формирующие знания и навыки по прикладному программированию микропроцессорных систем и устройств, автоматизированному проектированию и разработке радиоэлектронных устройств, используемые в интегрированных системах безопасности.

Ведущими техническими высшими учебными заведениями страны преподаются дисциплины: "Прикладные инженерные программы", "Микропроцессоры и микропроцессорные системы", "Программирование и реализация встроенных систем".

Складывается практика проведения аналитических исследований, научно-исследовательских и опытно-конструкторских работ, организации профильных конференций и семинаров, что отражает растущий интерес общества, научных кругов и субъектов информатизации к различным аспектам деятельности в сфере информационной безопасности.

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

Ключевые проблемы

1. В Республике Казахстан за период с 2010 по 2016 год плотность пользователей Интернета увеличилась с 36,1% до 75%, а количество пользователей мобильного Интернета с 3 миллионов 694 тысяч практически утроилось и достигло 10 миллионов 567 тысяч. Такое экспоненциальное увеличение числа пользователей Интернета повышает критичность и делает более ощутимыми последствия в случае отказов или вредоносного воздействия на технические средства.

Распространенность вредоносных программ для персональных компьютеров и мобильных устройств растет вместе с числом их пользователей. При этом подавляющее большинство пользователей не используют специализированное программное обеспечение для защиты своих персональных компьютеров, смартфонов, планшетов.

Этот фактор эксплуатируется "хакерами", что каждый день приводит к увеличению количества атак, нацеленных на заражение абонентских устройств вредоносным программным обеспечением.

В то время, как количество абонентских устройств, подключенных к Интернету, увеличивается и большинство пользователей продолжает игнорировать меры "цифровой гигиены" в отношении себя и принадлежащих им устройств, концепция "Интернета вещей" только усиливает проблему их безопасного использования.

Если традиционные электронные устройства, такие как персональные компьютеры и ноутбуки имеют возможности по установке и обновлению антивирусного программного обеспечения, то пользователи "Интернета вещей", часто даже не знают, как обезопасить их функционирование.

Такие устройства пока, в принципе, создаются без учета технологических рисков, что делает их потенциальными элементами вредоносных сетей, ("ботнет"), используемых для осуществления различных сетевых атак, направленных на потерю доступности информационных систем и влекущих для добросовестных пользователей отказ в обслуживании при оказании информационно-коммуникационных услуг.

Пренебрежение соображениями безопасности при использовании Интернет-ресурсов и социальных сетей ведет к повышенному риску для неприкосновенности частной жизни, несанкционированному использованию или модификации общедоступных персональных данных, а также разглашению персональных данных ограниченного доступа или их экстерриториальной доступности для преступных сообществ или разведывательных структур при их хранении на территории других государств.

Низкая правовая грамотность по вопросам информационной безопасности и отсутствие сформировавшихся потребностей в ее повышении у населения, работников сферы ИКТ и руководителей организаций создают питательную почву для развития правонарушений и преступлений в информационной сфере.

Отсутствие знаний о правовых ограничениях создает иллюзию дозволенности действий, нарушающих права и свободы других граждан, права обладателей авторских и смежных прав на программное обеспечение и влияющих на функционирование информационных ресурсов.

Таким образом, низкий уровень цифровой грамотности конечных пользователей в вопросах защиты персональных данных при отсутствии базовых знаний по общим методам распространения вредоносных компьютерных программ и программных продуктов (особенно "фишинговые" страницы поддельных интернет-магазинов и банков, распространение вирусных и "троянских" программ через "взломанные" сайты, скачивание нелицензионного ("пиратского") программного обеспечения) приводят к тысячам случаев, когда граждане Республики

Казахстан становятся жертвами, а принадлежащие им технические средства орудиями противоправного использования ИКТ.

2. Недостаточная осведомленность в методах защиты информации и низкая обеспеченность в системах информационной безопасности предприятий малого и среднего бизнеса, в том числе занятых в сфере оказания информационно-коммуникационных услуг, которые зачастую даже не могут оценить состояние принадлежащей информационно-коммуникационной инфраструктуры, приводят к большому количеству не анализируемых событий и инцидентов информационной безопасности, затрудняющих как профилактику технологических уязвимостей, так и борьбу с преступниками, использующими ИКТ как средство для совершения преступлений.

Кроме того, такие хозяйствующие субъекты представляют угрозу для других, в первую очередь, крупных предприятий или государственных органов и организаций, с которыми они работают в качестве партнеров или подрядчиков.

При этом, крупный частный и финансовый сектор склонен полагаться исключительно на собственные силы, недооценивая важность совместных усилий и отраслевых инициатив по формированию действительно безопасной среды операционной деятельности.

В тоже время низкая заинтересованность работодателей и отсутствие профессиональной конкуренции являются демотивирующим фактором для инициативного саморазвития практикующих специалистов в сфере информационной безопасности, а также создают предпосылки для занятия последних незаконными видами деятельности.

3. Существующая казахстанская модель школьного, средне-специального, высшего и послевузовского образования в области ИКТ, включая специализацию в сфере информационной безопасности, требует постоянного и тщательного анализа со стороны всех заинтересованных лиц (включая Министерство образования и науки Республики Казахстан, высшие учебные заведения и потенциальных работодателей) на предмет соответствия современным потребностям общества и тенденциям обеспечения безопасного развития информационных технологий в виду динамического развития данной области.

В частности, периодического пересмотра требуют образовательные и профессиональные стандарты, классификаторы специальностей, дисциплины, их контентное содержание и результаты обучения. Возникает необходимость разработки механизма, позволяющего более гибко реагировать на современные вызовы в области ИКТ. В виду того, что знания в данной области быстро устаревают, требуется периодическое подтверждение квалификации специалистов.

Из 93 высших учебных заведений, в которых готовят специалистов в сфере ИКТ, только 7 готовят специалистов по специальности "Системы

информационной безопасности". Из 32439 студентов, обучавшихся в 2015-2016 годах, в указанных высших учебных заведениях только 362 (1,1%) обучались по специальности "Системы информационной безопасности", из них по государственному заказу 226 человек. Плановый выпуск в 2016 году составил 85 выпускников.

В 2016-2017 учебном году по государственному заказу на подготовку специалистов по специальности "Системы информационной безопасности" выделено 40 мест, 2014-2015 году – 60 мест, 2015-2016 году – 60 мест.

В этой связи будет уделено повышенное внимание на профориентационную работу по специальности "Системы информационной безопасности", в том числе обращено внимание абитуриентов на актуальность данной специальности, потребность специалистов данного профиля в индустрии.

Прием абитуриентов на обучение по специальности "Системы информационной безопасности" на коммерческой основе в недостаточной мере продвигается и рекламируется. Специальные дисциплины лишены наполнения, необходимого для применения выпускниками в специальных государственных органах после завершения обучения.

В учебных программах не учитываются требования к знаниям, умениям и навыкам профессионального стандарта "Специалист по информационной безопасности", утвержденного Национальной палатой предпринимателей "Атамекен" и основанного на отраслевой рамке квалификации.

Как следствие, в сфере ИКТ существует нехватка специалистов по информационной безопасности, как в государственном, так и частном секторе.

4. Отечественный сектор IT-отрасли не вносит существенного практического вклада в программу диверсификации национальной экономики (менее 5 процентов продуктов из используемых в государственном секторе имеют казахстанское происхождение), а культура кибербезопасности, в том числе производственная культура в сфере разработки и использования продуктов, не всегда является определяющей.

Несмотря на достигнутый высокий уровень информатизации сферы государственного управления, включая оборону и безопасность, широкое использование ИКТ в различных сферах жизни личности и общества, Казахстан как страна, пока, в значительной мере импортирует (заимствует) не только IT-технологии, но и готовые программные продукты, включая продукты обеспечения информационной безопасности в сфере информатизации и связи, что указывает с одной стороны на давление со стороны гигантов IT-индустрии, а с другой на недостаточность принимаемых усилий и мер по их рациональному замещению с опорой на собственные силы в критически важных сферах разработок, от которых зависит обеспечение безопасности государства.

5. Меры, связанные с автоматизацией государственных функций и оказанием государственных услуг в электронной форме, а также продолжающаяся цифровизация доступа к информации о деятельности государственных органов несут в себе определенные риски.

Некачественные услуги и приложения, предоставляемые гражданам и частным организациям в рамках "электронного правительства", в том числе машиночитаемые открытые данные, могут привести к нарушению прав и законных интересов граждан.

Отклонения от установленных требований технических стандартов, вызванные низким уровнем производственной и эксплуатационной культуры, небрежность и халатность со стороны заказчиков и разработчиков решений на этапе создания, принцип остаточного финансирования обеспечения информационных систем системами защиты информации и контроля защищенности несут в себе высокие риски технологических сбоев.

Несвоевременное устранение владельцами информационных систем уязвимостей в программном обеспечении существенно увеличивает угрозы несанкционированного доступа.

Объем данных, обрабатываемых в государственном и частном секторах, растет, что приводит к необходимости выработки новых форм их хранения. В тоже время, такие формы хранения данных как облачное хранилище или использование онлайн-сервисов часто основываются операторами и поставщиками услуг на непрозрачных или не стандартизованных решениях, в том числе с точки зрения безопасности данных.

Ситуация усугубляется возможностью намеренного внедрения в программное обеспечение и телекоммуникационное оборудование не декларируемых функций (так называемых "бэкдоров"), которые не всегда могут быть выявлены на этапе сертификации, устранения уязвимостей в процессе эксплуатации или распознаны антивирусными программами и потому могут быть использованы для нарушения работы информационных систем и сетей телекоммуникаций.

6. Транснациональный и трансграничный характер многих продуктов ИКТ и международная связанность сетей телекоммуникаций общего пользования используются преступностью в целях совершения противоправных действий в отношении пользователей и операторов ИКТ-услуг и владельцев Интернет-ресурсов, размещенных в национальном сегменте, а также информационных систем, взаимодействующих с Интернетом.

Высокая латентность и зачастую международный характер таких преступлений повышают их общественную опасность. Ситуация усугубляется укоренившимися в обществе стереотипами о безнаказанности так называемой «киберпреступности», ненужности принимаемых государством мер по укреплению сферы безопасного использования ИКТ,

ограниченными возможностями органов правопорядка по привлечению к ответственности виновных в совершении высокотехнологичных преступлений, несмотря на развитые уголовно-правовые институты информационной безопасности.

7. Нагнетаемая отдельными странами милитаризация сферы ИКТ, трудности в доказывании причастности государств к использованию ИКТ в нарушение принципов международного права, вызванные в значительной степени стихийно сложившимся характером существующей международной системы управления Интернетом, сохраняющийся цифровой разрыв между странами препятствует формированию в мировом сообществе надежных международно-правовых инструментов предотвращения военного использования достижений в сфере информатизации и телекоммуникаций.

При этом по своей сути арсенал, используемый в военных целях, не отличается от арсенала программно-технических средств, используемых киберпреступностью, о чем свидетельствуют массовые случаи использования ИКТ в разведывательных, подрывных и иных целях, угрожающих поддержанию международного мира и безопасности.

Таким образом, Казахстан в сфере кибербезопасности испытывает такие серьезные угрозы как:

низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности;

нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере ИКТ установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме;

непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное обеспечение и другие элементы информационно-коммуникационной инфраструктуры;

действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг;

деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру.

3. Международный опыт

Термин "Кибербезопасность" и его производные (киберпространство, киберзащита, кибератаки, кибернападение и другие) не имеют единого общепризнанного юридического определения на международном уровне.

В тоже время на уровне ООН имеется ряд документов, таких как Глобальная программа кибербезопасности Международного союза электросвязи или Резолюция Генеральной Ассамблеи ООН "Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур", в которых содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования информационно-коммуникационных технологий в вопросах обеспечения (1) неприкосновенности частной жизни, (2) конфиденциальности, целостности и доступности информации в электронной форме, (3) защиты критической информационно-коммуникационной инфраструктуры, взаимодействующей с Интернетом (в том числе информационных систем, аппаратно-программных комплексов, телекоммуникационных систем, сетей телекоммуникаций, систем защиты информации, программного обеспечения) от вредоносного воздействия программно-техническими методами.

При этом многие страны не рассматривают в руководящих документах вопросы защиты от вредной или незаконной информации, распространяемой с использованием ИКТ в контексте понимания кибербезопасности из-за опасений в чрезмерном ограничении права на доступ и свободное распространение информации.

Отдельные страны рассматривают через призму кибербезопасности только неконтролируемое распространение в Интернете, как всемирной системе объединенных сетей телекоммуникаций и вычислительных ресурсов, электронных материалов, пропагандирующих терроризм, детскую порнографию и некоторые виды незаконной информации, в первую очередь, по причине технической сложности установления источника распространения такой информации.

При этом некоторые страны в оценке угроз и принимаемых в отношении них мер противодействия придерживаются понятия информационной безопасности применительно ко всем аспектам использования ИКТ, выстраивая соответствующую модель правового регулирования и системы государственного управления.

Так, например, стратегия Норвегии отмечает, что новые услуги и устройства предъявляют весьма высокие требования к компетенции простых пользователей. Но главная ответственность за обеспечение безопасности информации, систем и сетей возлагается на владельца или оператора. Такие работы должны быть частью ежедневной работы и финансироваться наряду с текущими операциями. Стоимость мер по содействию информационной безопасности должна быть соразмерна оценке риска в отдельных сферах управления (глобальный индекс кибербезопасности составляет 0,735).

Эстония придает особое значение безопасности информационных систем. Рекомендуемые меры носят гражданский характер и основываются

на правовом регулировании, обучении и сотрудничестве (глобальный индекс кибербезопасности составляет 0,706).

В основе стратегии Финляндии лежит понимание кибербезопасности как проблемы экономического характера, тесно связанной с развитием финского информационного общества (глобальный индекс кибербезопасности составляет 0,618).

Словакией обеспечение информационной безопасности рассматривается в качестве необходимого условия нормального функционирования и развития общества. Поэтому цель стратегии – служить прочным фундаментом для защиты информации. Стратегия направлена как на предотвращение угроз, так и на обеспечение готовности и устойчивости средств их предотвращения (глобальный индекс кибербезопасности составляет 0,618).

Ключевые цели стратегии кибербезопасности Чешской Республики включают в себя защиту информационно-коммуникационных систем от уязвимостей, которым эти системы подвергнуты, и уменьшение потенциального ущерба от атак на системы. Основной фокус стратегии приходится на проблемы свободного доступа к информационным сервисам, целостности и конфиденциальности данных в Чешской Республике (глобальный индекс кибербезопасности составляет 0,500).

Франция ориентируется на то, чтобы информационные системы были способны противостоять событиям, которые могут отрицательно повлиять на доступность, целостность и конфиденциальность информации, делает упор на технические средства защиты информации, борьбу с киберпреступностью и установлением киберзащиты (глобальный индекс кибербезопасности составляет 0,588).

Стратегия Германии закладывает основу для безопасности критически важных информационных систем. Германия сосредоточена на предотвращении и уголовном преследовании кибератак, а также выхода из строя IT-оборудования, вызванного случайными факторами. Стратегия кибербезопасности Германии определяет уровень кибербезопасности, достигнутый суммой всех национальных и международных мер, принятых для защиты и доступа к информации и коммуникациям, целостности, достоверности и конфиденциальности данных в киберпространстве, а также укреплением германского технологического суверенитета и экономического потенциала во всем диапазоне основных стратегических IT-компетенций (глобальный индекс кибербезопасности составляет 0,706).

Программа развития электронной информационной безопасности Литвы ориентируется на определении целей и мероприятий, направленных на обеспечение электронной информационной безопасности, развитие оборота электронной информации, а также обеспечение ее конфиденциальности, доступности и целостности в киберпространстве. Кроме того, стратегия Литвы направлена на защиту персональных данных,

телекоммуникационных сетей, информационных систем и критически важных инфраструктур от нарушения безопасности и кибератак из-за пределов "электронного периметра" (глобальный индекс кибербезопасности составляет 0,441).

Нидерланды, с одной стороны, стремятся к безопасным и надежным информационно-коммуникационным системам, опасаясь серьезных нарушений в этих системах, а с другой стороны, признают необходимость свободы и открытости Интернет-пространства. В стратегии дается определение кибербезопасности. "Кибербезопасность – это защищенность от сбоев и неправильной эксплуатации информационно-телекоммуникационных систем. Сбои и неправильная эксплуатация могут отрицательно повлиять на доступность и надежность информационно-телекоммуникационных систем, поставить под угрозу конфиденциальность и целостность информации, хранящейся в системах" (глобальный индекс кибербезопасности составляет 0,676).

Стратегия безопасности ИКТ Австрии заключается в распространении интегральных подходов к безопасности, реализованных в системе "электронного правительства", к другим областям, включая те, которые должны быть созданы на транснациональном уровне в целях обеспечения долгосрочной жизнеспособности экономики Австрии (глобальный индекс кибербезопасности составляет 0,676).

Подход Великобритании направлен на развитие кибербезопасности. Цель: вывести Соединенное Королевство на первое место по инновациям, инвестициям и качеству сервисов в сфере информационно-телекоммуникационных технологий, и тем самым, в полной мере воспользоваться всеми преимуществами и достоинствами киберпространства. Необходимо исключить риски типа кибератак преступников, террористов и других государств с целью сделать киберпространство безопасным для граждан и экономики (глобальный индекс кибербезопасности составляет 0,706).

Национальная стратегия Швейцарии отмечает необходимость уменьшения влияния преобладающих интересов нескольких стран, участвующих в Интернет-индустрии, рассматривает применение описываемых в ней мер "в мирное время, и тем самым, явным образом исключает войны".

При этом отказоустойчивая военная инфраструктура рассматривается как важный элемент стратегического резерва для других субъектов в случае полномасштабного кризиса. Поскольку действующее законодательство в различных отраслях отражает кибер-аспекты существующих задач и обязанностей государственного и частного сектора, решение вопросов кибербезопасности в рамках единого специального кибер закона Швейцарии считается непригодным, так как "непрерывно адаптироваться к изменениям

должно действующее законодательство" (глобальный индекс кибербезопасности составляет 0,353).

Таким образом, в каждой стране национальное понимание кибербезопасности и ключевых приоритетов значительно различается.

Как следствие, различаются и подходы к составлению стратегий кибербезопасности. Тем не менее, руководящие документы, охватывающие вопросы кибербезопасности, как правило, предусматривают:

- построение государственной системы управления в сфере обеспечения кибербезопасности;

- определение соответствующего механизма (в основном общественно-государственного партнерства), позволяющего частным и государственным заинтересованным сторонам обсуждать проблемы обеспечения безопасности национальных информационных инфраструктур;

- определение необходимой политики безопасности и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора (например, обязательное информирование об инцидентах безопасности, базовые меры обеспечения безопасности и руководства к действию, новые нормы материально-технического обеспечения).

Как свидетельствует мировой опыт, полную защиту от ошибок в программном обеспечении или инцидентов информационной безопасности достигнуть невозможно, но путем осознанного ответственного поведения снизить их частоту и вероятность, обеспечить высокую скорость восстановления работоспособности информационных систем и ресурсов, чтобы не допустить разрушительных последствий, жизненно необходимо.

Координация этой сферы во многих странах в значительной степени выстраивается вокруг гражданского регулятора в области информационных технологий и связи (Агентство информационной безопасности KISA - Корея, Центр информационной безопасности Министерства информационных технологий – Республика Узбекистан, и др.), либо органа, ответственного за защиту и безопасность информации (Бюро безопасности информационной техники – Германия, Агентство безопасности информационных систем при Министерстве обороны – Франция, Агентство национальной безопасности Чехии, Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, Оперативно-аналитический центр при Президенте Республики Беларусь, Служба специальной связи и защиты информации Украины. В Европейском союзе регулятором в этой сфере является Агентство информационной и сетевой безопасности).

4. Цели, задачи, ожидаемые результаты и период реализации

Целями Концепции являются достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и

внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.

Задачи Концепции:

1. Формирование необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов и систем кибербезопасности, направленных на блокирование и подавление вредоносного программно-технического воздействия и защищенного телекоммуникационного оборудования.

2. Совершенствование правоприменительной практики, методологической базы, нормативно-правового и организационно-технического обеспечения безопасного использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами.

3. Создание высоко адаптивной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно-коммуникационной инфраструктуры.

Ожидаемые результаты:

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

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

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

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

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

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

Период реализации Концепции включает два этапа:

1) первый этап 2017-2018 годы;

2) второй этап 2019-2022 годы.

На первом этапе будут:

- сформирована развернутая правоприменительная практика соблюдения уже установленных требований в сфере обеспечения информационной безопасности, по результатам которого будут внесены необходимые изменения в законодательство;

- проведена ревизия образовательных программ и профессиональных стандартов, увеличено количество и качество подготавливаемых специалистов в области информационной безопасности, обеспечено повышение квалификации действующих работников, занятых в этой сфере;

- выстроена эффективная схема взаимодействия и кооперации между промышленностью и наукой в создании отечественных разработок, что создаст основу для развития национального и отраслевых оперативных центров информационной безопасности, что позволит на втором этапе обеспечить:

- ключевое участие казахстанских IT-компаний в обеспечении национальной информационно-коммуникационной инфраструктуры системами информационной безопасности;

- загрузку отечественных предприятий электронной промышленности заказами на приобретение государственными органами и квазигосударственным сектором телекоммуникационного оборудования, произведенного и прошедшего процедуры сертификации на соответствие требованиям информационной безопасности на территории страны.

5. Основные принципы и подходы

Основные принципы:

1) соблюдение прав, свобод и законных интересов физических лиц, а также прав и законных интересов юридических лиц;

2) обеспечение безопасности личности, общества и государства при применении информационно-коммуникационных технологий;

3) осуществление деятельности по информатизации на территории Республики Казахстан на основе единых стандартов, обеспечивающих надежность и управляемость объектов информатизации;

4) четкое разграничение полномочий государственных органов;

5) непрерывный мониторинг информационной безопасности объектов информационно-коммуникационной инфраструктуры;

6) интеграция системы обеспечения национальной безопасности с международными системами безопасности.

Для реализации задачи по формированию необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов, систем информационной безопасности и телекоммуникационного

оборудования, устойчивых к вредоносному программно-техническому воздействию предлагается:

Формирование в обществе устойчивых представлений о "кибергигиене" и привитии высокой производственной культуры создания и использования ИКТ на всех этапах жизненного цикла программных продуктов, информационных систем, программного обеспечения, технологических платформ, информационной и сетевой инфраструктуры, поддерживающего оборудования.

Применение тренингов и обучающих практик по защите персональных данных и неприкосновенности частной жизни среди несовершеннолетних пользователей Интернета и их родителей.

Для профессионализации работников, ответственных за состояние информационной безопасности в государственных органах, и универсализации принимаемых ими мер соответствующим образом, адаптация профессиональных стандартов, а также расширение требований по практическим навыкам и техническим знаниям, улучшающим профили защиты и параметры контроля защищенности информационных ресурсов и систем.

Отведение важнейшей роли в реализации образовательных и исследовательских задач в сфере информационной безопасности высшими учебными заведениями Казахстана, что расширит технические возможности специальных государственных органов по обеспечению безопасности государства и повысит уровень аналитического и научно-исследовательского сопровождения мероприятий по реализации Концепции.

Решение задач по закладыванию и поддержанию высокого уровня профессиональной компетенции и технической готовности к противодействию киберпреступности путем привлечения научно-исследовательских организаций к участию в расследовании правоохранительными органами наиболее сложных киберпреступлений.

Для наращивания казахстанского потенциала в сфере научной, научно-технической и образовательной деятельности необходимо сосредоточиться на научно-исследовательских и опытно-конструкторских работах, обеспечить тесную связь учебного процесса с производственной деятельностью предприятий электронной промышленности, привести учебные программы в соответствие с отраслевыми профессиональными стандартами и современным уровнем развития технологий.

Предоставление приоритета исследованиям и собственной школе прикладной математики, по разработке средств криптографической защиты информации, криптологии, разработок по программируемым логическим интегральным схемам, квантовой криптографии и разработке защиты систем передачи, обработки и хранения информации, а также систем информационной безопасности.

Преодоление проблемы не высокой востребованности отечественных разработок, т.к. кибербезопасность в конечном итоге зависит от уровня развития отечественной IT-отрасли и электронной промышленности. Одной из причин этого является отсутствие обязательности приоритетного использования их продукции в государственных органах.

Установление мер по их поддержке, в том числе через стимулирование государственно-частного партнерства повышения конкурентоспособности. Критериями должны стать соответствие требованиям локализации разработки и технической поддержки, наличие у поставщика исключительных прав интеллектуальной собственности на конструкторскую и техническую документацию программных продуктов и телекоммуникационного оборудования, а также наличие научно-производственной базы, необходимой для организации производства, гарантийного и послегарантийного обслуживания.

Проведение совместно с представителями отрасли постоянного анализа закупаемого в государственных органах и квазигосударственном секторе программном обеспечении и телекоммуникационного оборудования с целью определения перспектив их замещения на доверенные отечественные или иностранные образцы, прошедшие процедуры обязательной сертификации на соответствие требованиям информационной безопасности.

При уполномоченном органе по информационной безопасности образовать Совет по кибербезопасности, одной из главных задач которого должно стать рассмотрение актуальных вопросов по кибербезопасности, поддержание в актуальном состоянии руководящих документов, нормативно-правовой базы, содействие приоритетному использованию продукции отечественной электронной и софтверной промышленности, проведение публичной оценки общественно-значимых IT-проектов.

Установление постоянного прямого диалога с ведущими компаниями и предприятиями страны, образовательными и научными исследовательскими организациями, что позволит объединить усилия и придать системность и комплексность решению задач по обеспечению интегрированной кибербезопасности в наиболее значимых областях использования ИКТ.

Наряду с мониторингом, анализом защищенности государственных информационных систем и ресурсов, оказания содействия по безопасному использованию ИКТ в интересах граждан, дополнительным приоритетом государственной службы реагирования на компьютерные инциденты KZ-CERT определить популяризацию мер "кибергигиены".

Соизмеряясь со своими экономическими возможностями, собственникам и владельцам частных информационных систем стремиться к следованию стандартизованным процессам разработки, создания, испытаний и эксплуатации информационных систем, предусматривая необходимые меры по обеспечению их информационной безопасности. Способные

выступить в качестве необходимого ориентира технические стандарты и другие нормативно-технические документы для этого имеются.

Для решения задачи по совершенствованию правоприменительной практики, методологической базы, нормативно-правового и организационно-технического обеспечения безопасного использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами предлагается:

Неукоснительное исполнение уже установленных законодательством и техническими стандартами требований по обеспечению информационной безопасности в государственном секторе, а также оперативное внесение в них необходимых изменений с учетом динамики развития технологий без ущерба для кибербезопасности.

Соблюдение установленных требований обеспечить действенными мерами государственного контроля.

Для полноценной оценки состояния защищенности объектов информатизации с учетом характера деятельности киберпреступников и иностранных технических компьютерных разведок, рассчитывающих на самоуспокоенность и небрежность со стороны владельцев информационных ресурсов и систем, необходимо стремиться к непрерывному мониторингу состояния информационных систем и ресурсов техническими средствами контроля защищенности и проведению работы по выявлению каналов утечки информации (уязвимостей, вирусов, троянских программ, недекларируемых функций и закладок).

Такой подход позволит обеспечить сохранение возможности реализации государственных функций в случае чрезвычайных происшествий технологического, социального характера, вызванных инцидентами информационной безопасности, угрожающими национальной и общественной безопасности, а в случае чрезвычайного или военного положения возможности использования устойчивой информационно-коммуникационной инфраструктуры сил обеспечения национальной безопасности в интересах функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

Наряду с выстраиванием работы с объектами критической информационно-коммуникационной инфраструктуры из числа стратегических и особо важных государственных объектов, объектов стратегических отраслей экономики, пересмотреть критерий отнесения к критически важным объектам информационно-коммуникационной инфраструктуры с возможностью отнесения к критически важным объектам, ориентированных на оказание информационно-коммуникационных услуг населению.

Распространять предупредительные и профилактические меры не только на государственные органы и собственников частных информационных систем, интегрируемых с государственными, но и на

владельцев промышленных предприятий, финансовых организаций и других категорий объектов экономики, имеющих автоматизированные технологические процессы, нарушение которых может негативно сказаться на экономическом развитии страны.

На основе Единых требований и действующих Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства" предусмотреть разработку руководящих документов, служащих ориентиром не только для государственного сектора, но и для объектов, находящихся в частной собственности, в целях эффективной локализации и предотвращения реализации угроз в общенациональном масштабе.

В целях поддержания высокого доверия граждан и бизнеса к оказываемым государственными органами услугам на законодательном уровне для поставщиков программных продуктов, услуг связи и иной информационно-коммуникационной инфраструктуры выработать меры по информационной безопасности для указания в соглашениях, конкурсной документации и технических спецификациях к приобретаемым продуктам и решениям по обязательной технической поддержке закупаемых товаров и услуг в течение не менее трех лет.

Предусмотреть требования в сфере обеспечения безопасности автоматизированных систем управления технологическими процессами и телекоммуникационного оборудования сетей телекоммуникаций общего пользования. Особое внимание должно быть обращено на инфраструктуру в системах жизнеобеспечения населения, топливно-энергетическом секторе, инфраструктуре связи и других.

Существенно углубить понимание относительно устойчивости элементов критической инфраструктуры национального сегмента Интернета и центров обработки данных (дата-центров), аппаратно-программных комплексов, обеспечивающих функционирование общедоступных электронных информационных ресурсов (Интернет-ресурсов).

Обеспечение надежной идентификации, аутентификации и регистрации действий пользователей в соединении с мерами обеспечения конфиденциальности их персональных данных снижает риск наиболее распространенных угроз, связанных с аутентичностью пользователей информационных систем и общедоступных электронных ресурсов, включая аппаратно-программные комплексы электронных средств массовой информации. Это позволит исключить в национальном сегменте фальсификацию в сфере электронной коммерции, электронных платежей, банковской деятельности и других информационно-коммуникационных услуг, оказываемых посредством Интернет-ресурсов.

Для создания высоко адаптированной и интегрированной системы государственного управления информационной безопасностью в сфере

информатизации и связи в отношении всей национальной информационно-коммуникационной инфраструктуры предлагается:

Государственным органам и поставщикам услуг принять риск-ориентированный подход к безопасности, уделяя первоочередное внимание усилиям, которые обеспечивают наиболее высокий уровень надежности создаваемых информационных систем в нормальном и внештатном режимах и устойчивости их к умышленным сбоям.

Расширить взаимодействие между ведомственными и отраслевыми структурами мониторинга и реагирования на инциденты информационной безопасности для оказания содействия владельцам информационных ресурсов и систем и взаимного оповещения о возникающих угрозах. Их участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования, проектирования, разработки и эксплуатации отраслевых информационных систем и сетей и стать опорными точками, определяющими устойчивость всей информационно-коммуникационной инфраструктуры страны.

Специализация служб реагирования на инциденты информационной безопасности позволит расширить круг вовлеченных организаций и экспертов, что будет способствовать росту профессионализации работников, занятых в сфере информационной безопасности с учетом отраслевой специфики, и содействовать расширению рынка услуг аудита информационной безопасности для малого бизнеса, который часто не имеет возможности содержать квалифицированных специалистов в области IT и информационной безопасности.

Компьютерные атаки, запущенные из зарубежного пространства, максимально предотвращать на "электронной границе" - виртуальном периметре страны.

Руководящие документы Единой сети телекоммуникаций Республики Казахстан с учетом ее растущей уязвимости в результате конвергенции сетей телекоммуникаций и информационно-коммуникационных сетей и необходимости снижения объемов вредоносного трафика и своевременного блокирования операторами связи аномальной сетевой активности необходимо актуализировать.

Создание условий для эффективной борьбы с киберпреступностью путем постоянного повышения квалификации личного состава специализированных подразделений, расширения арсенала технических средств фиксации и криминалистических исследований "цифровых" доказательств.

Обеспечение кибербезопасности является задачей всех субъектов, деятельность которых связана с использованием ИКТ, поэтому сотрудничество в целях обеспечения информационной безопасности будет способствовать защите интересов всех заинтересованных сторон.

Для объединения усилий при участии научного сообщества, частного сектора подготовить создание Национального координационного центра информационной безопасности, который в онлайн режиме будет обрабатывать информацию о состоянии защищенности "электронной границы", а также наиболее важных компонентов национальной информационной инфраструктуры и обеспечить обмен информацией, что позволит:

обеспечить гражданам и бизнесу доступ к квалифицированным оценкам угроз в сфере информационной безопасности и получению дополнительных знаний о том, как уменьшить негативное влияние от угроз использования уязвимостей в программном обеспечении и информационных и телекоммуникационных системах;

Министерству внутренних дел снизить количество и обеспечить высокую раскрываемость в значительной степени латентных преступлений, совершаемых с использованием информационных технологий;

государственным органам поддерживать высокий уровень отказоустойчивости и предупреждения возникновения технологических сбоев, а также своевременного устранения их последствий в инфраструктуре, входящей в состав "электронного правительства" и других государственных информационных систем и ресурсов;

собственникам критически важных объектов информационно-коммуникационной инфраструктуры получать своевременную информацию о возможном влиянии на безопасность принадлежащих им автоматизированных систем управления технологическими процессами;

Национальному Банку и банкам второго уровня получать дополнительную информацию об актуальных угрозах финансово-банковской системе.

Министерству обороны в рамках развития военной организации страны подготовить предложения по созданию системы по эффективной защите ведомственных информационных ресурсов, прогнозированию и своевременному выявлению компьютерных атак, проводить их оценку и классификацию на предмет угрозы военной безопасности государства.

На внешнеполитическом и внешнеэкономическом уровне последовательно продвигать национальные интересы Республики Казахстан, направленные на преодоление "цифрового" разрыва между участниками международного сообщества в информационной сфере, обозначив в качестве приоритетов реализацию инициатив по укреплению, на основе норм и принципов международного права, системы международной информационной безопасности.

В рамках двух и многосторонней дипломатии продолжить укреплять роль Казахстана в качестве сильного и последовательного партнера, выступающего против использования ИКТ в военных целях, следующего курсу открытости, укрепления мер доверия в области международной

информационной безопасности, при безусловном соблюдении суверенного равенства государств в выборе путей технологического развития. Ключевыми диалоговыми площадками должны стать международные, региональные и субрегиональные организации (ООН, ШОС, ЕАЭС, ОДКБ, СНГ и др.) с дальнейшим продвижением их инициатив в различных международных форматах.

Скоординированная реализация Концепции "Киберщит Казахстана" позволит существенно повысить место Казахстана в Глобальном индексе кибербезопасности и достигнуть к 2022 году индекса 0,600.

Необходимые ресурсы

На реализацию Концепции в 2017-2022 годах будут направлены средства государственного бюджета в рамках бюджетных программ заинтересованных государственных органов и предусмотренных в Плане реализации Государственной программы "Цифровой Казахстан 2020".

6. Перечень нормативных правовых актов, посредством которых предполагается реализация Концепции

В период реализации данной Концепции достижение поставленных целей и задач предполагается посредством следующих нормативных правовых актов:

1. Уголовный кодекс Республики Казахстан от 3 июля 2014 года.

2. Кодекс Республики Казахстан "Об административных правонарушениях" от 5 июля 2014 года.

3. Предпринимательский кодекс Республики Казахстан от 29 октября 2015 года.

4. Закон Республики Казахстан от 15 сентября 1994 года "Об оперативно-розыскной деятельности".

5. Закон Республики Казахстан от 31 августа 1995 года "О банках и банковской деятельности в Республике Казахстан".

6. Закон Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи".

7. Закон Республики Казахстан от 5 июля 2004 года "О связи".

8. Закон Республики Казахстан от 27 июля 2007 года "Об образовании".

9. Закон Республики Казахстан от 18 февраля 2011 года "О науке".

10. Закон Республики Казахстан от 6 января 2012 года "О национальной безопасности Республики Казахстан".

11. Закон Республики Казахстан от 21 мая 2013 года "О персональных данных и их защите".

12. Закон Республики Казахстан от 11 апреля 2014 года "О гражданской защите".

13. Закон Республики Казахстан от 16 мая 2014 года "О разрешениях и уведомлениях".

14. Закон Республики Казахстан от 24 ноября 2015 года "Об информатизации".

15. Закон Республики Казахстан от 4 декабря 2015 года "О государственных закупках".

16. Указ Президента Республики Казахстан от 8 января 2013 года № 464 "О Государственной программе "Информационный Казахстан – 2020" и внесении дополнения в Указ Президента Республики Казахстан от 19 марта 2010 года № 957 "Об утверждении Перечня государственных программ".

17. Постановление Правительства Республики Казахстан от 23 августа 2012 года № 1080 "Об утверждении государственных общеобязательных стандартов образования соответствующих уровней образования".

18. Постановление Правительства Республики Казахстан от 23 мая 2016 года № 298 "Об утверждении Правил проведения аттестации информационной системы, информационно-коммуникационной платформы "электронного правительства", Интернет-ресурса государственного органа на соответствие требованиям информационной безопасности".

19. Постановление Правительства Республики Казахстан от 8 сентября 2016 года № 529 "Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры".

20. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности".

21. Приказ Министра по инвестициям и развитию Республики Казахстан от 29 января 2015 года № 66 "Об утверждении Единых правил взаимодействия и централизованного управления сетями телекоммуникаций.

22. Приказ Министра по инвестициям и развитию Республики Казахстан от 25 декабря 2015 года № 1240 "Об утверждении Правил выдачи сертификата безопасности".

23. Приказ Министра по инвестициям и развитию Республики Казахстан от 25 декабря 2015 года № 1241 "Об утверждении Правил применения сертификата безопасности".

24. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 25 января 2016 года № 60 "Об утверждении Правил взаимодействия государственных органов по вопросам соблюдения требований законодательства Республики Казахстан в сетях телекоммуникаций".

25. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66 "Об утверждении Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства".

26. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 63 "Об утверждении методики и правил

проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", Интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности".

27. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 67 "Об утверждении Правил оказания услуг доступа к Интернету в пунктах общественного доступа к Интернету".

28. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 65 "Об утверждении Правил присоединения сетей операторов междугородной и международной связи к точке обмена Интернет-трафиком".

29. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 108 "Об утверждении Методики проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы "электронного правительства", Интернет-ресурса государственного органа на соответствие требованиям информационной безопасности".

30. Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 118 "Об утверждении Правил регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета".

Калиев А.А. Киберпреступность в современном мире: основные понятия и тенденции. Учебное пособие. - г.Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2023. – 103 с.

Подписано в печать «___».___.2023 г. Формат 60Х84/16
Усл. печ. л. ____. Тираж 15 экз. Заказ №_____

Отпечатано в типографии
Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан
г. Косшы, ул. Республики, строение 94