Impact Factor: 9.9 ISSN-L: 2544-980X

Влияние Киберпреступлений На Безопасность Человека

МЕ Санаев [1], Эльмуродова Фарида Фаридовна [2]

Киберпреступность, киберправо и киберэтика

Киберпреступность-это преступная деятельность, *совершаемая* против компьютеров или других устройств или с их помощью. Наиболее распространенными видами киберпреступлений являются компьютерное пиратство, онлайн-мошенничество, атаки на компьютерные системы, кража личных данных и распространение незаконной или запрещенной информации.

При совершении киберпреступлений основными целями считаются:

- незаконное приобретение денег, ценных бумаг, кредитов, материальных ценностей, товаров, услуг, льгот, недвижимости, топливного сырья, энергоносителей и стратегического сырья;
- отказ от уплаты налогов и различных сборов;
- отмывание денег;
- фальсификация или изготовление поддельных документов, штампов, печатей, бланков, квитанций за личные достижения;
- получение конфиденциальной информации в личных или политических целях;
- месть на почве лично враждебных отношений с начальством или коллегами по работе;
- вмешательство в денежную систему страны в личных или политических целях;
- дестабилизация ситуации в стране, территориально-административном устройстве или регулирование в политических целях;
- грабеж, уничтожение противника или нарушение порядка работы учреждения, предприятия или системы в политических целях;
- для сокрытия других видов преступлений;
- в исследовательских вопросах;
- для демонстрации личных интеллектуальных способностей или превосходства.
- Мотивами резкого роста объемов киберпреступлений являются:
- выход из финансовых затруднений;
- незамедлительно взыскать с общества долг, причитающийся преступнику;
- преследование компании и работодателя;
- показать себя неравным.

Виды киберпреступности. Строго классифицировать виды киберпреступлений невозможно. Поэтому ниже будут представлены виды киберпреступлений, относящиеся к сфере криминологии. В литературе, связанной с криминологией, выделяют следующие виды киберпреступлений:

- экономические компьютерные преступления;
- против конституционных прав и свобод человека и гражданина ;

[1] Самаркандский филиал международной школы финансовых технологий и науки
[2] Самаркандский филиал международной школы финансовых технологий и науки Студент

- компьютерные преступления против общественной и государственной безопасности.

Экономические компьютерные преступления широко распространены на практике. Они приносят преступникам миллионы долларов нелегальной прибыли. Самым распространенным среди них является мошенничество. Мошенничество в основном осуществляется через банковские счета и банковские карты. В международной практике к преступлениям, совершаемым с использованием пластиковых карт, относятся утеря или кража карт, создание или использование поддельных платежных карт, получение и незаконное использование информации о банковском счете без предъявления карты, а также владельцем карты, связанные с совершенными преступлениями.

Еще одним видом киберпреступности является «компьютерное пиратство» — преступления против прав и свобод человека и гражданина. Эти преступления проявляются в незаконном копировании, использовании и распространении программного обеспечения. Это серьезно наносит ущерб правовым отношениям (авторским правам), связанным с созданием программного обеспечения и базы данных. Это также причиняет огромные финансовые потери компаниям-разработчикам программного обеспечения.

Григор Барсегян, директор Microsoft в Армении, заявил, что ущерб, причиненный производителям "компьютерным пиратством", составляет 66 миллиардов долларов в год. По его словам, армянские потребители сознательно используют программы с высоким риском заражения вирусом, чтобы сэкономить свои финансовые ресурсы.

Последний тип компьютерных преступлений — это компьютерные преступления против общественной или национальной безопасности, которые включают в себя действия, опасные для общества, направленные на общественную или общественную безопасность, и часто связанные с нарушениями правил передачи данных, системы обороны страны или связанных с ней нарушений. распад его компонентов.

Киберетика

Киберэтика — это философская область, связанная с компьютерами, которая изучает поведение пользователей, то, на что запрограммированы компьютеры, и как они влияют на людей и общество в целом. Примеры проблем киберэтики включают в себя:

- Можно ли делиться личной информацией о других людях в Интернете (например, онлайн-статусами или текущим местоположением по GPS)?
- нужно защитить пользователей от фейковой информации?
- кому принадлежит цифровая информация (музыка, фильмы, книги, веб-страницы и т. д.) и какие права на нее имеют пользователи;
- Какой уровень азартных игр и порнографии должен быть в сети?
- Должен ли каждый иметь возможность пользоваться Интернетом?

Свойство. Споры по поводу этики использования информации уже давно касаются концепции собственности. Это стало причиной множества конфликтов в сфере киберэтики. Споры о собственности возникают, когда права собственности нарушены или неясны.

Права интеллектуальной собственности. Непрерывный рост Интернета и появление различных технологий сжатия данных (например, mp3) проложили путь для однорангового обмена файлами. Хотя эта технология впервые появилась в таких программах, как Napster, теперь она позволяет пользователям анонимно передавать файлы друг другу, используя протоколы передачи данных, такие как BitTorrent. Хотя большая часть транслируемой музыки защищена авторским правом, этот метод сделал ее распространение среди других незаконным.

Сегодня большинство электронных медиафайлов (музыка, аудио и фильмы) распространяются среди общественности без соблюдения прав интеллектуальной собственности. Например, в результате выхода «пиратских» версий большинства фильмов, на которые были потрачены большие деньги, бывают случаи, когда они не могут покрыть свои расходы.

Это можно увидеть и в отношении программного обеспечения. Например, хотя большинство программ считаются лицензионными, их «взломанные» версии широко используются на практике различными методами. Проблемы, нелицензионная ОС Windows 10, антивирусное ПО, офисное ПО и взлом.

Технические средства защиты авторских прав. При защите авторских прав используются различные методы защиты. Они могут включать в себя что угодно: от защиты данных CD/DVD от несанкционированного копирования до ограничения возможности редактирования простых файлов PDF. Однако другая категория людей считает, что если я куплю лицензионный компакт-диск, то у меня также будет возможность копировать с него.

Безопасность. Безопасность при использовании информации в Интернете уже давно стала темой этических дебатов. Это поднимает вопрос о защите общественного благосостояния или защите прав личности в первую очередь. В результате увеличения числа пользователей Интернета и увеличения персональных данных увеличивается количество краж и киберпреступлений.

Ясность. Из-за присутствия Интернета и характера отдельных лиц или групп проблема точности информации становится проблемой. Другими словами, кто несет ответственность за достоверность информации в Интернете? Кроме того, возникают споры о том, кто заполняет информацию в Интернете и кто должен нести ответственность за ошибки и упущения в ней.

Юзабилити, цензура и фильтрация. Темы удобства использования, цензуры и фильтрации информации поднимают множество этических проблем, связанных с киберэтикой. Существование этих проблем ставит под сомнение наше понимание конфиденциальности и конфиденциальности, а также наше участие в жизни общества. Любой закон может ограничить использование информации или запретить распространение или использование такой информации на основе фильтрации. Цензура также может быть низкого уровня (например, компания для собственных сотрудников) или высокого уровня (вводится государством в целях обеспечения безопасности). Одним из лучших примеров того, как управлять данными, поступающими в страну, является проект, известный как Великий китайский файрвол.

Свобода информации. Свобода информации, то есть свобода слова, наряду со свободой искать, получать и распространять информацию, ставит вопрос о том, кто и что поможет при кибератаке? Право на свободу информации обычно подвергается ограничениям, которые затрагивают затрагиваемую страну, общество или культуру. Ограничения могут принимать различные формы. Например, в некоторых странах Интернет является формой доступа к средствам массовой информации и используется всеми жителями страны. Кроме того, ограничения на использование Интернета в некоторых штатах могут различаться от штата к штату.

Цифровые барьеры. Отдельной проблемой, помимо этических вопросов, связанных со свободой информации, является так называемый *цифровой барьер* . Это относится к социальному разрыву между теми, кто имеет ограниченный доступ или ограниченный доступ к цифровым и информационным технологиям, таким как киберпространство. Этот разрыв между странами или регионами мира называется глобальным цифровым разрывом.

Запрещенный контент (порнография). Использование несовершеннолетними запрещенного контента в Интернете всегда является источником этических дискуссий. В некоторых странах использование такого контента строго запрещено, а в других разрешено.

Азартные игры. Эта проблема также является одной из дискуссионных в этическом вопросе, и некоторые считают ее вредной, а другие не поддерживают вмешательство закона. В свою очередь, между этими партиями ведется дискуссия о том, какие виды игр следует разрешить? Где их следует проводить? Эти вопросы вызывают широкие дискуссии. В настоящее время в большинстве стран есть законное разрешение на игры такого типа, а в других действуют строгие ограничения.

Этика использования компьютера. Институт компьютерной этики — некоммерческая организация, миссией которой является продвижение технологий с этической точки зрения. Эта организация цитирует следующие 10 правил этики:

- не используйте свой персональный компьютер во вред другим;
- не мешать работе на компьютере других пользователей;
- не просматривайте компьютерные файлы других людей;
- не используйте компьютер для кражи;
- не используйте компьютер во зло;
- не используйте и не копируйте программное обеспечение, которое вы не приобретали;
- не использовать чужой компьютер без разрешения;
- не вредить плодам интеллектуального труда других;
- подумайте о социальных последствиях создаваемой вами программы;
- используйте свой компьютер осознанно и с уважением к другим.

Кодекс разумного использования информации. Кодекс разумного использования информации основан на пяти принципах, которые подчеркивают требования к системе бухгалтерского учета. Эти требования были введены Министерством здравоохранения и социальных служб США в 1973 году:

- не должно быть систем сбора персональных данных;
- каждый человек должен контролировать, какая информация о нем хранится в системе и как она используется;
- каждый человек должен иметь возможность предотвратить использование собранной о нем информации как в одних, так и в других целях;
- каждый должен исправить информацию о себе;
- Каждая организация, которая создает, хранит, использует или распространяет коллекцию персональных данных, должна гарантировать, что эти данные используются только для тех целей, для которых они предназначены, и принять меры против их использования в других целях.

Кибер-законы

Национальные законы. 12 декабря 2002 года был принят Закон Республики Узбекистан № 439-II «О принципах и гарантиях свободы информации». Этот закон состоит из 16 статей. В частности, оно определяет следующее:

Статья 1. Основные задачи настоящего Закона

Основными задачами настоящего Закона являются обеспечение соблюдения принципов и гарантий свободы информации, реализация прав каждого свободно и беспрепятственно искать, получать, проверять, распространять, использовать и хранить информацию, а также защиту информации и информационная безопасность личности, общества и государства состоит из верховой езды.

Статья 4. Свобода информации

Согласно Конституции Республики Узбекистан каждый имеет право беспрепятственно искать, получать, проверять, распространять, использовать и хранить информацию.

Доступ к информации может быть ограничен только в соответствии с законом и в целях защиты прав и свобод человека, основ конституционного строя, моральных ценностей общества,

духовного, культурного и научного потенциала страны, а также в целях защиты обеспечить его безопасность.

Статья 6. Открытость и раскрытие информации

Информация должна быть открытой и прозрачной, за исключением конфиденциальной информации.

Конфиденциальная информация не включает: правовые документы о правах и свободах граждан, порядке их реализации, а также правовом положении органов государственной власти и управления, органов самоуправления граждан, общественных объединений и других негосударственных некоммерческих организаций;

сведения об экологической, метеорологической, демографической, санитарно-эпидемиологической, чрезвычайной ситуации и другие сведения, необходимые для обеспечения безопасности населения, населенных пунктов, производственных объектов и коммуникаций;

доступная информация в открытых фондах информационно-библиотечных учреждений, архивов, ведомственных архивов и информационных систем юридических лиц, действующих на территории Республики Узбекистан.

Органы государственной власти и управления, органы самоуправления граждан, общественные объединения и иные негосударственные некоммерческие организации обязаны информировать средства массовой информации о событиях, фактах, явлениях и процессах, затрагивающих интересы общества, в соответствии с порядком установлено законом.

Статья 10. Отказ предоставить информацию

Если запрашиваемая информация является конфиденциальной или в результате ее разглашения могут быть нарушены права и законные интересы человека, интересы общества и государства, в предоставлении информации может быть отказано.

Уведомление об отказе в предоставлении запрашиваемой информации будет направлено лицу, обратившемуся с запросом, в течение пяти дней со дня получения запроса.

В уведомлении об отказе должна быть указана причина невозможности предоставления запрошенной информации.

Субъект конфиденциальной информации обязан уведомить владельца запрашивающей информацию о действующих ограничениях на получение этой информации.

Лица, которым незаконно было отказано в информации, а также лица, получившие по их запросу недостоверную информацию, имеют право на возмещение причиненного им материального ущерба или на компенсацию морального вреда в соответствии с законом.

Статья 11. Защита информации

Любая информация должна быть защищена, если ее незаконное обращение может причинить вред владельцу информации, собственнику, пользователю информации и иному лицу.

Защита данных:

предотвращение угроз информационной безопасности личности, общества и государства;

обеспечение конфиденциальности информации, предотвращение ее распространения, хищения, утраты;

проводится в целях предотвращения искажения и фальсификации информации.

13- вещество Безопасность личной информации

Информационная безопасность человека обеспечивается путем создания необходимых условий и гарантий для свободного использования им информации, сохранения тайны, связанной с его

личной жизнью, защиты от незаконного психологического воздействия в средствах массовой информации.

Личная информация, относящаяся к физическим лицам, классифицируется как конфиденциальная информация.

Разрешить собирать, хранить, обрабатывать, распространять и использовать информацию, касающуюся частной жизни физического лица, без его согласия, а также информацию, нарушающую тайну частной жизни, переписки, телефонных переговоров, почты, телеграфа и иную тайну связи, за исключением тайны связи. случаях, предусмотренных законом.

Запрещается использовать информацию о физических лицах в целях причинения им материального и морального вреда, а также воспрепятствования реализации их прав, свобод и законных интересов.

Граждане о информация получатель , такой к информации собственность делатель и от него пользователь юридический и физический люди этот из информации использовать заказ нарушение для в законе иметь в виду пойманный способ ответственный будет

Средства массовой информации не имеют права раскрывать источник информации или псевдонима автора без их согласия. Источник информации или имя автора могут быть раскрыты только по решению суда.

14- вещество Информационная безопасность общества

Информационная безопасность общества достигается следующими способами: обеспечение развития основ демократического гражданского общества, свободы публичной информации;

не позволять средствам информации незаконно влиять на общественное сознание, отвлекать его;

сохранение и развитие духовного, культурного и исторического богатства общества, научного и научно-технического потенциала страны;

создание системы действий против информационной экспансии, направленной на подрыв осознания национальной идентичности, отчуждение общества от исторических и национальных традиций и обычаев, дестабилизацию общественно-политической ситуации, нарушение межнационального и межконфессионального согласия.

15- вещество Информационная безопасность государства

Информационная безопасность государства обеспечивается следующими способами: осуществлением экономических, политических, организационных и иных мер против угроз информационной безопасности;

сохранение государственной тайны и защита государственных информационных ресурсов от их несанкционированного использования;

Интеграция Республики Узбекистан в мировое информационное пространство и современные телекоммуникационные системы;

Насильственное изменение конституционного строя Республики Узбекистан, нарушение территориальной целостности, суверенитета, узурпация власти или смещение законно избранных или назначенных представителей власти и иная агрессия против государственного строя

защита от распространения информации, включающей явные вымогательства; действовать против распространения информации, в том числе пропаганды войны и насилия, жестокости, распространения идей терроризма и религиозного экстремизма, направленных на разжигание социальной, национальной, расовой и религиозной вражды.

16- вещество Ответственность за нарушение законодательства о принципах и гарантиях

свободы информации

Лица, виновные в нарушении законодательства о принципах и гарантиях свободы информации, привлекаются к ответственности в установленном порядке.

Ответственность за борьбу с киберпреступностью в Республике Узбекистан перечислена ниже.

Кодекс об административной ответственности Республики Узбекистан: *Статья 155. Нарушение правил использования информации*

Нарушение правил использования информации и информационных систем, выражающееся в несанкционированном доступе к информационной системе в целях ее использования.

влечет наложение штрафа в размере от одной трети до единовременного размера минимальной заработной платы на граждан, а также от одного до трехкратного размера минимальной заработной платы на должностных лиц.

То же нарушение, повлекшее нарушение работы информационных систем, а равно непринятие соответствующих мер защиты при подключении информационных систем с ограниченным доступом к информационным и вычислительным сетям, -

влечет штраф на граждан от одного до трех минимальных размеров оплаты труда, на должностных лиц - от трех до пяти минимальных размеров оплаты труда.

Незаконное подключение информационных систем юридических и физических лиц к международным информационным сетям, подключение к этим сетям без принятия соответствующих мер защиты, а равно незаконное получение от них данных.

влечет наложение штрафа от двух до пяти минимальных размеров оплаты труда на граждан и от пяти до семи минимальных размеров оплаты труда на должностных лиц.

Публикация от своего имени чужой программы или базы данных, созданных для электронно-вычислительных машин, а также их незаконное копирование или распространение таких произведений - наказываются штрафом в размере от одного до трех минимальных размеров оплаты труда для граждан и от трех до пяти минимальных размеров оплаты труда для должностных лиц. причина

Статья 218. Незаконное изготовление и распространение продукции СМИ Незаконное изготовление и распространение продукции средства массовой информации без регистрации в установленном порядке или после принятия решения о прекращении ее выпуска или опубликования - наказываются конфискацией печатной или иной продукции и штрафом в размере от трех до пяти минимальных размеров оплаты труда.

Уголовный Кодекс Республики Узбекистан:

Статья 143. Нарушение тайны переписки, телефонных переговоров, телеграфных сообщений или иных сообщений.

Умышленное нарушение тайны переписки, телефонных переговоров, телеграфных сообщений или иных сообщений, совершенное после применения за такие действия административного взыскания, - штраф в размере до двадцати пяти минимальных месячных заработных плат или до трех лет, наказываются лишением определенных прав или обязательными общественными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до трех лет.

Безопасность человека

Социальная (социальная) инженерия – это совокупность различных психологических методов и мошеннических практик, целью которых является получение обманным путем конфиденциальной информации о человеке. Конфиденциальная информация — это имена пользователей/пароли, личная информация, компромат, номера банковских карт и любые финансовые или репутационные данные.

Этот термин пришел из области хакерства. *Хакер* – это человек, который ищет уязвимости в компьютерной системе, иначе говоря – «разрушитель». Насколько социальная инженерия может быть актуальна в этом случае.

Сегодня хакеры понимают, что главной уязвимостью любой системы является не машина, а человек. Человек, как и компьютер, работает по определённым законам. Хакеры начали «атаковать людей», используя накопленный человечеством опыт в рамках психологии, приемы и механизмы воздействия. Иногда их называют «майнд-хакингом».

Пример. Предположим, хакер хочет забрать у вас деньги. Допустим, у него есть информация о вашем номере телефона и аккаунте в социальной сети. Кроме того, он также узнал из розыска, что у вас есть брат, и собрал достаточно информации и о вашем брате. Он также добавил номер телефона твоего брата. После этого, основываясь на этой информации, он начал строить свой план.

План: Хакер позвонит вам вечером и представит (возможно, какой-нибудь лич, который называет вас только вашим братом вместо вашего имени), что я ваш брат и что он столкнулся на улице с бандитами, которые украли все его вещи. (телефон, деньги, пластиковая карта и т.п.). Кроме того, он говорит, что ему помогла девушка, но денег у него с собой не было. При этом эта девушка имеет при себе пластиковую карту и требует перевести на эту пластиковую карту 20 000 сумов, необходимых для того, чтобы добраться до больницы. Хакерам это удается в 8/10 случаев, и опытному хакеру сделать это несложно.

В этом случае можно говорить о возможности отделения голоса вашего брата. Однако человек может находиться в среде с разным волнением и шумом! Кроме того, если у вас есть телефон, пока вы спите, вам будет сложнее распознать голос.

Давайте посмотрим на идеи, использованные хакером в данном случае:

1. Хорошо скрытый человек и на реальных примерах (например, ваши фотографии, места, которые знают только ваши близкие и т. д.) и придумал хорошую легенду.
2. Все это сказано быстро и достаточно убедительно.
3. Был использован очень большой механизм воздействия – воздействие на жалость (обращение к эмоциям).

Список использованных литератур

1. Eshquvvat o’g’li M.S, Zafar qizi Z.B Areas of application of artificial intelligence issn: 2181-4027 sjif: 4.995 Volume-27, Issue-2, February-2023. 61-64.
2. Eshquvvat o’g’li M.S, Naim o‘g‘li M. D, Xamrobek o’g’li N.N, Data miningda crisp-dm metodoligiyasi tasnifi Часть-11_ Том-1_ Декабрь-2023 43-46.
3. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. Обратная задача по определению кинетического коэффициента в модели фильтрац ii tom tatu sf ma’ruzalar to‘plami 9 aprel 2022-yil 11-13.
4. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. Идентификация коэффициента кинетики в модели фильтрации суспензии в пористой среде халқаро илмий-амалий анжуман материаллари 2022 йил, 11-12 май 360-361.
5. Eshquvvat o'g'li.M.S, Shodiyor o'g'li.Sh.J, Raxmonqul o'g'li.A.T, Ma'lumotlarni sinflashtirishda birch algoritmi ahamiyati Часть-11 Том-1 Декабрь -2023 39-42.
6. ME Sanayev, AA Quchqorov Classification of computer application software, European journal of business startups and open society Дата 2024/3/10, том 4, номер 3, страницы 62-65.
7. ME Sanayev, OF Orifov method oriented practical software classification Miasto Przyszłości 46, 210-213.

8. ME Sanayev, OF Orifov The role of text editors in editing and processing text information, European journal of innovation in nonformal education 4(3),43-47
9. SM Eshquvvat o'g'li, Kompyuter amaliy dasturiy ta'minoti tasnifi, Journal of new century innovations 48 (1), 3-8.
10. ME Санаев, КТ Бегмаматов, Топология и современные типы компьютерных сетей, Журнал, Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
11. ME Sanayev, The role, purpose and functions of information and communication technologies and systems in the economy in the process of modern education, Журнал, Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
12. ME Sanayev, Comparative analysis of the windows operating system, Журнал, Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17, Номер 1.
13. ME Sanayev, AI Ismoilov, Analysis of modern operating systems, Журнал Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
14. ME Sanayev, MB Shaymanov, Modern information technology infrastructure parts, Журнал Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
15. ME Sanayev, AI Ismoilov, The development tendencies of software products in the management of business processes in the economy, Журнал Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17, Номер 1.
16. ME Sanayev, FS Tovbayev, Familiarity with the basic concepts and features of the windows operating system, Журнал Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17 Номер 1.
17. ME Sanayev, Mobil operasion tizimlar tahlili, Журнал "germany" modern scientific research: achievements, innovations and development prospects, Дата 2024/4/20 Том 17 Номер 1.
18. ME Sanayev, AA Quchqorov, The Role of Social Networks in Human Life, Miasto Przyszłości 46, 340-341.
19. SM Eshquvvat o'g'li, Kompyuter dasturiy ta'minotiga bo'lgan talablarini tizimli tahlil qilish, Miasto Przyszłości 46, 262-265.
20. ME Sanayev, Kiber xafsizlik tushunchasi va uning vazifalari, Экономика и социум, 613-619.
21. ME Sanayev, Identifikasiya va autentifikatsiya, Экономика и социум, 620-626.