

*Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:*

<https://studservis.ru/gotovye-raboty/referat/324393>

**Тип работы:** Реферат

**Предмет:** Информационные системы и процессы

Введение 3

1. Понятие о киберпреступности и киберпреступлениях 4

2. Классификация киберпреступлений 5

3. Методы борьбы с киберпреступностью 10

4. Киберпреступления в наше время 13

5. Статистика киберпреступлений 15

Заключение 16

Список использованных источников 17

Введение

Применение информационных технологий распространяется на все аспекты человеческой деятельности, от наблюдения за воздушным и наземным транспортом до решения проблем национальной безопасности. Информация является важнейшим компонентом этого процесса и приобретает все большее значение для отдельных людей, обществ и наций. В результате информационная безопасность рассматривается как неотъемлемый элемент государственной безопасности.

К сожалению, развитие научно-технического прогресса (НТП), сопровождающее внедрение современных информационных технологий, привело к появлению новых форм преступной деятельности. К ним относятся незаконное вмешательство в электронные компьютеры, системы и сети, а также кража, присвоение, вымогательство компьютерных данных и другие рискованные антиобщественные действия, которые в совокупности именуется «киберпреступностью».

Эксперты утверждают, что последствия использования информационных систем в преступных целях аналогичны последствиям применения оружия массового уничтожения. Таким образом, киберпреступность признается быстро растущей угрозой безопасности как для отдельных стран, так и для мирового сообщества. Следовательно, борьба с киберпреступностью стала главным приоритетом, и суды все чаще рассматривают дела, связанные с этим видом преступлений.

Цель работы:

Исследование киберпреступности и киберпреступлений как потенциальной угрозе современному обществу.

Задачи работы:

1. Дать определение понятиям «киберпреступность» и «киберпреступления»;
2. Дать общую характеристику киберпреступности и киберпреступлениям;
3. Выделить основные разновидности киберпреступлений;
4. Дать описание киберпреступлениям в наше время;
5. Определить основные правила компьютерной безопасности;
6. Привести статистику киберпреступлений.

1. Понятие о киберпреступности и киберпреступлениях

Киберпреступность — это преступная деятельность, происходящая в виртуальном пространстве.

Виртуальное пространство, или киберпространство, можно описать как моделируемое компьютером информационное пространство, содержащее данные о людях, объектах, фактах, событиях, явлениях и процессах, представленные в символической или иной форме. Эти данные передаются по локальным и глобальным компьютерным сетям или хранятся на физических или виртуальных устройствах и других носителях, предназначенных для хранения, обработки и передачи.

Преступление, совершаемое в киберпространстве, представляет собой незаконное вмешательство в работу ЭВМ, программ для ЭВМ и сетей ЭВМ, несанкционированное изменение данных ЭВМ и иные общественно опасные действия, связанные с использованием ЭВМ, сетей ЭВМ и программ. Киберпреступность охватывает широкий спектр правонарушений, включая преступления, связанные с компьютерами, такие как мошенничество, когда компьютеры используются в качестве инструментов или средств для совершения преступлений против собственности, авторского права, социального обеспечения или нравственности.

Киберпреступность не ограничивается национальными границами, и международные организации сыграли фундаментальную роль в ее определении и борьбе с ней. В 2001 году Совет Европы принял Конвенцию о борьбе с киберпреступностью, которая установила правовую основу для расследования и судебного преследования за киберпреступления. В соответствии с этой конвенцией киберпреступность включает преступления против конфиденциальности, целостности и доступности компьютерных систем, сетей и информации, а также незаконное использование этих систем, сетей и данных. Киберпреступность — это подкатегория компьютерных преступлений, которая включает преступления, совершенные с использованием Интернета или других компьютерных сетей как часть преступления.

Существуют различные типы киберпреступлений, некоторые из которых связаны с прямыми атаками на компьютеры или другие устройства с целью их вывода из строя. Другие предполагают использование компьютеров в злонамеренных целях, таких как распространение вредоносного кода, кража информации или получение криптовалюты. Разделить киберпреступность на отдельные категории сложно из-за множества разновидностей преступления.

## 2. Классификация киберпреступлений

Конвенция Совета Европы о киберпреступности, также известная как Будапештская конвенция о киберпреступности, определяет четыре категории преступлений, связанных с компьютерными системами и данными, которые она определяет следующим образом:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем: в эту категорию входят такие правонарушения, как незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему и неправомерное использование устройств.

2. Преступления, связанные с компьютером: в эту категорию входят такие правонарушения, как подлог и мошенничество, совершенные с использованием компьютерных систем, а также правонарушения, связанные с контентом, такие как детская порнография.

3. Правонарушения, связанные с контентом: в эту категорию входят правонарушения, связанные с незаконным контентом, такие как разжигание ненависти, расизм и ксенофобия.

4. Правонарушения, связанные с нарушением авторских и смежных прав. В эту категорию входят правонарушения, связанные с несанкционированным воспроизведением и распространением материалов, защищенных авторским правом, таких как музыка, фильмы и программное обеспечение.

Конвенция обеспечивает основу для международного сотрудничества в расследовании и судебном преследовании таких видов киберпреступлений, а также поощряет разработку эффективного национального законодательства по борьбе с киберпреступностью.

Концепция киберпреступности была рассмотрена на Десятом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, который состоялся в Вене, Австрия, в апреле 2015 года. Конгресс признал растущую важность борьбы с киберпреступностью, которая стала серьезной угрозой для отдельных лиц, предприятий и правительства по всему миру.

В ходе Конгресса участники обсудили широкий круг вопросов, связанных с киберпреступностью, в том числе проблемы расследования и уголовного преследования киберпреступников, необходимость международного сотрудничества в борьбе с киберпреступностью, а также важность защиты прав и свобод человека в Интернете.

Конгресс также принял «Венскую декларацию о преступности и правосудии: ответы на вызовы 21 века», в которой признается необходимость комплексного и комплексного подхода к предотвращению киберпреступности и борьбе с ней. Декларация призвала государства-члены укреплять свои правовые рамки и потенциал правоохранительных органов для борьбы с киберпреступностью, а также содействовать международному сотрудничеству и наращиванию потенциала в этой области.

В целом Десятый Конгресс ООН по предупреждению преступности и уголовному правосудию сыграл важную роль в повышении осведомленности об угрозе, которую представляет собой киберпреступность, и в содействии международному сотрудничеству в борьбе с этой растущей проблемой.

1. Агаркова А. А., Сеницына В. А. Киберпреступность в современной России. Международный журнал гуманитарных и естественных наук, 2021. № 5-3. С. 13-16.

2. Бондарь Е. О. Киберпреступность как новая криминальная угроза. Вестник Московского университета МВД России, 2020. № 1. С. 155-158.

3. Дерюгин Р. А. Киберпреступность в России: современное состояние и актуальные проблемы. Вестник Уральского юридического института МВД России, 2019. № 2. С. 46-49.

4. Кириленко В. П., Алексеев Г. В. Киберпреступность и цифровая трансформация. Теоретическая и прикладная юриспруденция, 2021. № 1 (7). С. 39-53.
5. Ковтун К. А. Банковская киберпреступность как одна из основных проблем современного общества. Теоретическая и прикладная юриспруденция, 2021. № 1 (7). С. 94-97.
6. Кувшинова В. С. Криминологическая характеристика киберпреступности. Международный журнал гуманитарных и естественных наук, 2020. № 5-4. С. 53-57.
7. Купирова Ч. Ш., Кузьмин Ю. А. Информационная безопасность как объект киберпреступности. Oeconomia et Jus, 2019. № 4. С. 41-46.
8. Лакомов А. С. Киберпреступность: современные тенденции. Академическая мысль, 2019. № 2 (7). С. 53-56.
9. Лобач Д. В., Смирнова Е. А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам. Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса, 2019. № 4 (11). С. 23-32.
10. Мальцева А. П., Лошкарев А. В. Влияние цифровой экономики на киберпреступность. Международный журнал гуманитарных и естественных наук, 2019. № 10-2 (37). С. 117-120.
11. Приходько А. А., Керопян Г. Б. Потери банков от киберпреступности. StudNet, 2020. Т. 3. № 12. С. 212-217.

*Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:*

<https://studservis.ru/gotovye-raboty/referat/324393>