МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

Нижегородский государственный педагогический университет им. К. Минина

Факультет информационных технологий

«правонарушения в сфере информационных технологий»

Реферат

по дисциплине

Информатика

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Балунова С.А.

(подпись)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гусева Е.А.

(подпись)

ИСТ-23-2

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Содержание**

1. 1 глава
   1. Информационное общество. Современные сквозные информационные технологии.
   2. Что такое современное информационное общество?
   3. Достоинства и недостатки
   4. Что такое сквозные информационные технологии?
   5. Как искусственный интеллект используется в теме вашего реферата.
2. 2 глава
   1. Определение
   2. Основные характеристики
   3. Классификация
   4. Историческая справка
   5. Как использовать в жизни
   6. Анализ ПО
3. Вывод
4. Список литературы

1 глава.

Информационное общество. Современные сквозные технологии.

Сквозные цифровые технологии- передовые научно-технические отрасли, обеспечивающие создание высокотехнологичных продуктов и сервисов, наиболее сильно влияющих на развитие экономики

К сквозным цифровым технологиям относятся:  
технологии виртуальной и дополненной реальности, квантовые технологии, новые производственные технологии, технологии беспроводной связи, система распределенного реестра, компоненты робототехники и сенсорика, нейротехнологии и искусственный интеллект.

Технология виртуальной реальности позволяет с помощью специальных устройств погрузить человека в некое подобие окружающего нас мира. Создаваемые эффекты воспринимаются с помощью зрения, слуха, осязания. А технология дополненной реальности дает возможность открыть интерактивный контент и увидеть виртуальный 3D-объект с анимацией или видео, которым можно управлять в реальном пространстве.

Квантовые технологии предполагают использование особенностей квантовой механики для проведения сложных расчетов с наибольшей эффективностью, а также обеспечить абсолютную защищенность информации за счет квантовой запутанности частиц.

К новым производственным технологиям относятся цифровое проектирование, математическое моделирование, технологии "умного" производства.

Технологии беспроводной связи включают в себя глобальную сеть связи, сети локальной связи, сети, связывающие разные устройства, используемые человеком, а также технологии передачи связи между космосом и землей.

Системы распределенного реестра представляют собой децентрализованные системы, в которых пользователи совместно используют защищенный от несанкционированного доступа общий реестр операций в виде цепочки блоков. Доступ к реестру есть у всех пользователей системы. Каждый блок является закодированным набором информации, а последующий блок содержит код предыдущего блока. Например, если кто-то хочет провести ложную операцию (изменить какой-либо блок), то мгновенно изменится код всех блоков. Соответственно, операция не будет проведена.

Сквозная технология "компоненты робототехники и сенсорика" включает в себя разработку автоматизированных технических систем, сенсорных систем и методов обработки сенсорной информации, взаимодействия технических систем между собой и с человеком.

К нейротехнологиям относятся нейропротезирование, технологии распознавания потребительской информации путем нейроинтерфейсов, нейростимуляции и другие.   
Искусственный интеллект дает возможность освободить человека от ряда работ, включая опасные, помогает принимать решения и упрощает коммуникацию между людьми.

Что такое современное информационное общество?

Понятие информационного общества уже давно не ново и изучено. Оно было впервые предложено японским теоретиком К. Коямой, и его труды послужили основой для принятия программы "План информационного общества: национальная цель к 2000 году" в Японии. Концепция информационного общества отличалась тем, что впервые введен четвертый сектор - информационный, который являлся главным и системообразующим в обществе. Кояма отметил, что информация стала ключевым фактором производства. При этом, несмотря на преобладание информационных ресурсов, традиционные индустрии продолжали развиваться, удовлетворяя первичные потребности людей. С течением времени, западные страны также стали использовать термин "информационное общество" с 1992 года. Информационное общество - это общество, в котором большинство людей занято производством, хранением, переработкой и распространением информации. Знания становятся его высшей формой, а информация - объектом всеобщего потребления. Основными признаками информационного общества являются: рост роли информации и знаний, увеличение числа работников в сфере информационных технологий, рост доли информационных продуктов и услуг в экономике, появление глобального информационного пространства, развитие информационной экономики, электронного правительства, социальных сетей и цифровых рынков. Главное отличие информационного общества заключается в растущей роли информации, которая становится основным ресурсом и самым быстрорастущим сектором в обществе.

Достоинства и недостатки

Информация и знания становятся главными продуктами информационного общества. Эта концепция характеризуется ростом роли информации, знаний и информационных технологий в общественной жизни. Всё больше людей занято информационными технологиями, коммуникациями и производством информационных продуктов и услуг. Телефония, радио, телевидение, интернет, а также традиционные и электронные СМИ все шире используются.   
Самая важная особенность заключается в создании глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам и удовлетворение их потребностей в информационных продуктах и услугах. Также активно развиваются электронная демократия, информационная экономика, электронное государство, электронное правительство, цифровые рынки, электронные социальные и экономические сети. Можно сказать, что электронные технологии становятся главным связующим звеном в мире.  
Одним из важных преимуществ стала возможность управления крупными организациями и системами, требующими координации деятельности сотен тысяч и даже миллионов людей. Всё больше внимания уделяется проблемам организационных структур и развитию новых научных направлений.  
Однако информатизация общества несет и неприятные аспекты, такие как утрата устойчивости в информационном пространстве. В силу важности информации, небольшие группы людей могут оказывать существенное влияние на остальное население, например, через террор. Проблема устойчивости информационного общества может быть решена путем усиления учетных политик, включая развитие биометрии и криптографии.

Что такое сквозные информационные технологии?

«Сквозные» цифровые технологии (СЦТ) – это инновационные технологии, применяемые для электронного сбора, хранения, обработки, поиска, передачи и представления информации. Они основаны на использовании программных и аппаратных средств и систем, которые охватывают все сферы экономики и общественной жизни. «Сквозные» цифровые технологии не только преобразуют существующие бизнес-процессы и рынки, но и способствуют возникновению новых. Для того, чтобы экономика перешла на новый уровень и стала «цифровой», требуется взаимодействие и взаимопроникновение ключевых «сквозных» технологий, которые изменяют функциональные возможности бизнеса, социальной сферы и предприятий. Данное сотрудничество способствует приданию экономическим процессам нового качества и престижа.

Как искусственный интеллект используется в правонарушениях в сфере информационных технологий

Использование искусственного интеллекта в работе правоохранительных органов, особенно в борьбе с преступностью, является актуальным и востребованным. Программное обеспечение позволяет фиксировать и предупреждать правонарушения, а также быстро реагировать на них. Некоторые из возможностей включают распознавание лиц через системы видеонаблюдения, использование беспилотников для обнаружения преступлений и обеспечения безопасности на дорогах, установку стационарных технических средств для фиксации правонарушений на дорогах, а также создание прогнозов преступности для оптимизации работы правоохранительных органов. Искусственный интеллект также активно применяется в создании автоматизированных систем и баз данных, которые помогают в поиске преступников и защите потенциальных жертв преступлений.

2 глава

Определение

Информационное правонарушение – это противоправное и виновное действие или бездействие, которое является общественно опасным и совершается в сфере информации или других областях человеческой деятельности с использованием информационных систем.  
Основные признаки информационного правонарушения:  
1. Общественная опасность.  
2. Противоправность.  
3. Виновность деяния.  
Специальные признаки информационного правонарушения отличают его от других правонарушений:  
1. Совершаются в сфере информации, таких как поиск, передача, защита, хранение и использование информации, а также в других областях человеческой деятельности, например имущественные правонарушения, неимущественные, в области конституционного права личности, в области государственного управления или в ходе избирательных кампаний. При этом используются информационные системы, поэтому информационные правонарушения имеют двойную природу.  
2. Совершаются с помощью вспомогательных средств, что облегчает достижение поставленных целей.  
  
Общественная опасность информационного правонарушения может иметь разный уровень и степень (количественный и качественный признак).  
Виновность информационного правонарушения может выражаться в умышленной или неосторожной форме вины, включая утрату тайны.  
Объектом посягательства информационного правонарушения чаще всего является компьютерная информация, но также могут быть затронуты и другие элементы информационной системы, такие как объект посягательства и средство совершения преступления (статья 272, 274 Уголовного кодекса РФ в новой редакции).

Основные характеристики

Нарушением законодательства в сфере информации могут являться нарушения, связанные с обработкой информации, документированием информации и использованием компьютерной информации.  
Регулирование информационных правоотношений является сложным в связи с применением различных видов ответственности, включая административную, гражданско-правовую, уголовную и дисциплинарную.  
Объективная сторона нарушения заключается во внешнем проявлении незаконных действий в отношении информации. Она включает следующие признаки:  
1) Нарушение законодательных норм в сфере информации путем совершения или бездействия;  
2) Причинение вреда информационным интересам личности, общества или государства или создание реальной опасности такого вреда;  
3) Наличие причинной связи между незаконными действиями в сфере информации и последствиями в виде вреда информационным интересам.  
Субъективная сторона может быть выражена в умышленном или неосторожном нарушении. Уголовный кодекс РФ делит умысел на прямой и косвенный (ст. 25), а неосторожность - на легкомыслие и небрежность (ст. 26).  
Субъектами нарушения законодательства в сфере информации могут быть физические и юридические лица в зависимости от вида юридической ответственности. Российская правовая система предусматривает четыре вида ответственности для физических лиц за нарушение закона - дисциплинарную (включая материальную), административную, гражданско-правовую (имущественную) и уголовную.  
Юридические лица (предприятия, учреждения и организации) привлекаются только к административной и гражданско-правовой ответственности.

Классификация

Распространение вредоносных программ наказывается в соответствии со статьей 273 УК РФ. Существуют различные способы защиты, такие как использование проверенных сайтов, антивирусных программ, проверка съемных носителей и избегание подозрительных ссылок. Борьба с вредоносными программами осуществляется удалением с помощью антивирусных программ. Фишинг — вид мошенничества, цель которого — получение доступа к конфиденциальным данным. Это противозаконно по статье 272 УК РФ. Для защиты от фишинга рекомендуется проверять ссылки и не вводить личные данные на подозрительных сайтах. Взлом паролей также наказывается согласно статье 272 УК РФ. Чтобы предотвратить взлом, важно не отправлять личные данные третьим лицам, использовать сложные пароли и изменить логины и пароли после взлома. Кража банковских реквизитов — тяжкое преступление, наказываемое соответствующей статьей УК РФ. Кража может осуществляться через мобильный банк, с помощью мобильного телефона, смс-мошенничества, через интернет или с использованием поддельных банкоматов.

Историческая справка

За последние 10-15 лет количество преступлений, связанных с использованием вычислительной техники и электронной аппаратуры, значительно увеличилось. Они включают в себя хищение денежных средств и негласное получение информации. В России число компьютерных преступлений выросло в 22,3 раза за последние 10 лет, при этом годовой ущерб составляет около 613,7 млн. рублей. Расследование и предотвращение этих преступлений остается сложным заданием для правоохранительных органов. В основном, преступления совершают молодые люди возрастом от 18 до 25 лет с высшим образованием или его частью. Развитие компьютерной преступности обусловлено различными факторами, включая экономические, социальные и правовые. По мнению большинства респондентов, с ростом компьютеризации общества количество компьютерных преступлений будет увеличиваться, особенно в секторах смешанной и государственной экономики, а также в банковской и финансовой отраслях.

Как использовать в жизни

Как вычислить телефонного мошенника?

Чаще всего мошенники представляются сотрудниками службы безопасности банков или правоохранительных органов. Звонящий сообщает о попытке взлома или блокировки банковской карты, подозрительных действиях в интернет-банке, пропущенном платеже по кредиту или угрозе штрафа по надуманному обвинению. На самом деле сотрудники служб безопасности банков никогда не звонят клиентам, а о подозрительной деятельности или других проблемах сообщают другими способами.

Как вести себя во время разговора с незнакомым человеком?

Получив звонок от незнакомого человека, обратите внимание на то, что и как он хочет вам сообщить. Мошенники стремятся теми или иными способами надавить на жертв — торопить, запутывать, угрожать возможными последствиями. В такой ситуации важно сохранять спокойствие. Даже если вам угрожают потерей всех денег на счетах, не спешите выполнять требования звонящего. Также мошенник может несколько раз подряд задавать жертве вопросы, на которые можно ответить только словом «да». Столкнувшись с такими вопросами, старайтесь давать другие ответы, переспрашивать или переводить тему. Если вам звонят из банка — попробуйте задать уточняющие вопросы, например, о состоянии счета или последних операциях по карте. Скорее всего, злоумышленник ничего не сможет ответить. Если вам предлагают какую-либо выплату — уточните основание, на котором она производится.

Какую информацию нельзя сообщать собеседнику по телефону?

Мошенники стремятся получить секретные данные карты — трёхзначный код CVC/CVV с обратной стороны, коды подтверждения из SMS, логины и пароли от интернет-банков. Настоящие сотрудники банка никогда не запрашивают эту информацию — для обеспечения безопасности они используют отдельные технические средства. Для отправки платежа нужен только номер карты — другие данные для этого не нужны.

Как составить заявление по факту мошенничества по телефону?

Если вы столкнулись с телефонным мошенничеством — как можно скорее обратитесь в полицию, даже если вы не отправляли деньги или данные карты. В заявлении подробно опишите обстоятельства происшествия — время звонка номер телефона, ФИО и «должность» звонящего, содержание и итог разговора, если вы переводили деньги — отправленную сумму. В качестве основания укажите статью 159 УК РФ (если мошенник смог получить от вас деньги) и часть 3 статьи 30 УК РФ (если этого сделать не удалось). Если у вас есть запись звонка (его можно записать с помощью специального приложения) — приложите ее к заявлению.

Заявление будет рассматриваться в течение 10-30 дней. По итогам будет принято решение о возбуждении уголовного дела. Если вы получили отказ, то можно обжаловать его в прокуратуре — для этого потребуются копия заявления и постановление об отказе.

Анализ ПО

Выявляется вирус не сразу: первое время компьютер “вынашивает   
инфекцию”, поскольку для маскировки вирус нередко используется в   
комбинации с “логической бомбой” или “временной бомбой”. Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации.  Начиная действовать (перехватывать управление), вирус дает команду   
компьютеру, чтобы тот записал зараженную версию программы. После этого   
он возвращает программе управление. Пользователь ничего не заметит, так   
как его компьютер находится в состоянии “здорового носителя вируса”.   
Обнаружить этот вирус можно, только обладая чрезвычайно развитой   
программистской интуицией, поскольку никакие нарушения в работе ЭВМ в   
данный момент не проявляют себя. По оценке специалистов в “обращении” находится более 100 типов  вирусов. Варианты вирусов зависят от целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например,   
замедление в выполнении программ или появление светящейся точки на   
экране дисплея (т. н. “итальянский попрыгунчик”). Признаки могут быть   
иволютивными, и “болезнь” будет обостряться по мере своего течения. Так,   
по непонятным причинам программы начинают переполнять магнитные диски, в результате чего существенно увеличивается объем программных файлов.   
     Наконец, эти проявления могут быть катастрофическими и привести к   
стиранию файлов и уничтожению программного обеспечения.

Вывод

Информационное общество, основанное на современных сквозных информационных технологиях, принесло с собой как достоинства, так и недостатки. Оно обеспечивает быстрый и удобный доступ к информации, способствует развитию экономики и облегчает повседневные задачи, но одновременно создает уязвимость и риски, связанные с возможностью правонарушений.  
В современном информационном обществе, где информация является ключевым активом, возникают различные виды правонарушений. Под сквозными информационными технологиями понимаются такие технологии, которые пронизывают нашу повседневную жизнь и имеют широкий спектр применения. Они используются практически во всех сферах деятельности, включая образование, медицину, бизнес, правительство и т.д.  
Одним из недостатков современных информационных технологий является рост числа правонарушений, связанных с их использованием. Нарушение авторских прав, киберпреступления, нарушения конфиденциальности и безопасности данных становятся все более распространенными. С этим связана необходимость разработки соответствующего законодательства и механизмов защиты информации.  
Использование искусственного интеллекта в сфере информационных технологий является двуединой ситуацией. С одной стороны, искусственный интеллект способен обнаруживать и предотвращать правонарушения, улучшая безопасность и защищая данные от несанкционированного доступа. С другой стороны, искусственный интеллект может быть использован злоумышленниками для совершения нового поколения киберпреступлений, таких как социальная инженерия и заражение систем вредоносными программами.  
Для борьбы с правонарушениями в сфере информационных технологий необходимо развивать специализированные методы и технологии. Важно создание эффективных механизмов защиты данных, обучение пользователей об основных угрозах и правилами безопасного использования информационных технологий.  
В заключение, современные сквозные информационные технологии исключительно важны и полезны для развития информационного общества. Однако, они также требуют повышенного внимания и защиты от возможных правонарушений. Эффективные механизмы защиты, адекватное законодательство и осознанное использование информационных технологий соблюдение правил и этика вносят значимый вклад в обеспечение безопасности информационного общества в целом.

Список литературы.

* University Digital : сайт. – Тюмень, 2021. – URL: https://digital.tyuiu.ru/chto-takoe-skvoznye-tehnologii-i-pochemu-za-nimi-budushhee/ (дата обращения: 09.01.2024)
* Шашлова, С. А. Информационное общество и его основные черты / С. А. Шашлова. — Текст : непосредственный // Молодой ученый. — 2022. — № 17 (412). — С. 276-278. — URL: https://moluch.ru/archive/412/90772/ (дата обращения: 09.01.2024).
* Олеся Филиппова, Информационное общество: плюсы и минусы: портал / Омский экономический институт – Омск, 2014. – URL: https://sibadvokat.ru/magazine/sovety-advokata/informacionnoe-obshchestvo?ysclid=lr6svbr14c188523285 (дата обращения: 09.01.2024)
* Татьяна Шкляр.Сквозные цифровые технологии // Образовательный портал «Справочник». — Дата написания статьи: 08.07.2019. — URL https://spravochnick.ru/informacionnye\_tehnologii/skvoznye\_cifrovye\_tehnologii/ (дата обращения: 09.01.2024).
* Пшиченко Д.В. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ // Вестник науки №6 (63) том 1. С. 925 - 932. 2023 г. ISSN 2712-8849 // Электронный ресурс: [https://www.вестник-науки.рф/article/8698](https://www.xn----8sbempclcwd3bmt.xn--p1ai/article/8698) (дата обращения: 09.01.2024 г.)
* Лекция 8. ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ : сайт. – URL: https://eor.dgu.ru/lectures\_f/Информационное право курс лекций/Лекция 8.htm (дата обращения: 09.01.2024)
* Попов Алексей, Правонарушения в области информационных технологий, 30 дек 2022, сайт. – URL: [Правонарушения в области информационных технологий — Попов Алексей на vc.ru](https://vc.ru/u/1393633-popov-aleksey/574746-pravonarusheniya-v-oblasti-informacionnyh-tehnologiy?ysclid=lr6tsspmw4847692456) (дата обращения: 09.01.2024)